f

FUAA80000

ERRICHTERANLEITUNG

Comfion Funk-Sicherheitssystem

Deutsch English Français Nederlands

V2.0

1. Allgemeines

1.1. Einführung

Vielen Dank, dass Sie sich mit dem **Comfion Funk-Sicherheitssystem** für ein Produkt von ABUS Security Center (in der Kurzform auch "ABUS" genannt) entschieden haben.

Das vorliegende Handbuch enthält wesentliche Beschreibungen, Technischen Daten, Übersichten und weiterführende Informationen zur Projektierung, Inbetriebnahme und Bedienung des **Comfion Funk-Sicherheitssystems.**

Die hier beschriebenen Produkte/Systeme dürfen nur von Personen installiert und gewartet werden, die für die jeweilige Aufgabenstellung qualifiziert sind. Qualifiziertes Personal für die Installation und Wartung des Systems ist i. d. R. ein geschulter ABUS-Fachpartner.

1.2. Bestimmungsgemäße Verwendung / Rechtliche Hinweise

Die Verantwortung für den rechtskonformen Einsatz des Produkts liegt beim Käufer bzw. Kunden und dem Endnutzer. Gemäß der im Produkthaftungsgesetz definierten Haftpflicht des Herstellers für seine Produkte sind die vorstehenden Informationen zu beachten und an die Betreiber und Nutzer weiterzugeben. Die Nichtbeachtung entbindet ABUS Security Center von der gesetzlichen Haftung.

Nicht vereinbarungsgemäße bzw. unübliche Verwendung, nicht ausdrücklich von ABUS zugelassene Reparaturarbeiten bzw. Modifikationen sowie nicht fachgemäßer Service können zu Funktionsstörungen führen und sind zu unterlassen. Jegliche, nicht ausdrücklich von ABUS zugelassene, Änderungen führen zu Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.

Architekten, Technische Gebäudeplaner (TGA) und weitere beratende Institutionen sind angehalten, alle erforderlichen Produktinformationen von ABUS einzuholen, um den Informations- und Instruktionspflichten gemäß Produkthaftungsgesetz nachzukommen. Fachhändler und Verarbeiter sind angehalten, die Hinweise in der ABUS-Dokumentation zu beachten und diese gegebenenfalls an ihre Kunden weiterzuleiten.

Weiterführende Informationen finden Sie auf www.abus.com auf der allgemeinen Seite oder für Händler und Installateure im Partnerportal auf https://partner-asc.abus.com/

1.3. Kundendienst / Customer Support

Für weitere Hilfe steht unser Support-Team für Sie zur Verfügung: support@abus-sc.com

Allgemeine Informationen zum **Comfion Funk-Sicherheitssystem** finden Sie auf unserer Homepage unter:
https://www.abus.com/de/Privat/Alarmsysteme/Comfion-Funk-System

1.4. Impressum

1. Ausgabe Deutsch 05/2024

Mit dem Erscheinen einer neueren Installationsanleitung verliert diese Ausgabe ihre Gültigkeit.

Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernimmt ABUS Security Center keine Haftung. Die Angaben in dieser Installationsanleitung wurden nach bestem Wissen und Gewissen unter Berücksichtigung des jeweiligen Standes der Technik zusammengestellt. Sie werden regelmäßig überprüft und bei Bedarf aktualisiert bzw. korrigiert.

Alle Warenzeichen und Schutzrechte werden anerkannt, Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigungen vorgenommen werden.

1.5. Symbolerklärung

In dieser Installationsanleitung werden die folgenden Symbole verwendet:

Symbol	Signalwort	Bedeutung
	Vorsicht	Weist auf eine Verletzungsgefahr oder Gesundheitsgefährdung durch elektrische Spannung hin
	Wichtig	Weist auf eine mögliche Beschädigung des Geräts/Zubehörs oder auf eine Verletzungs- oder Gesundheitsrisiko hin
	Hinweis	Weist auf wichtige Informationen hin

2. Funktionsprinzip und Leistungsmerkmale

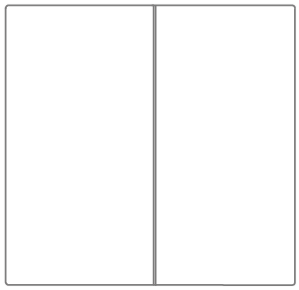
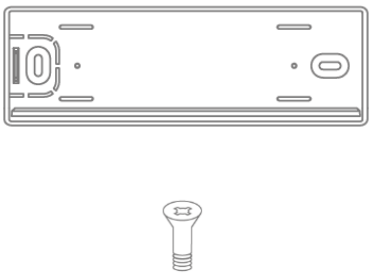
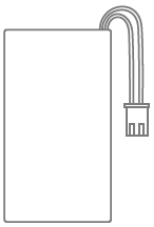
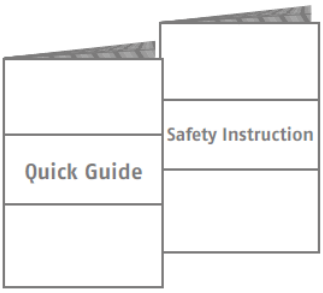
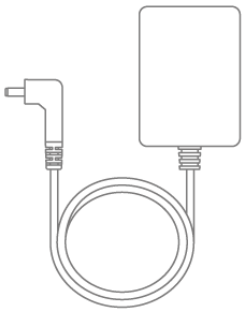
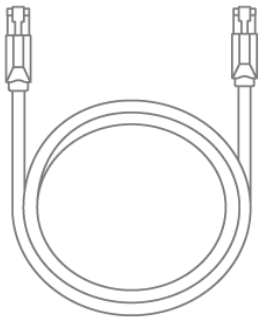
2.1. Produktmerkmale

Das **FUAA80000 Comfion Funk-Sicherheitssystem** ist ein EN-Grad-2-zertifiziertes Sicherheitssystem mit Smart Home-Funktionen. Das System kann über die intuitive App oder das ABUS Cloud-Portal eingerichtet und bedient werden.

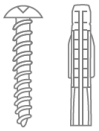
Hauptmerkmale:

- Einfache Montage: Eine Nachrüstung ist Dank Funk jederzeit mit wenig Aufwand möglich
- Integrierter NVR: Videoaufzeichnung mit bis zu 4 Kameras auf SD-Karte oder 4 Kanal-NVR direkt in der Zentrale, Einbindung tiefenintegrierter ABUS Professional Line Kameras
- Sicherer 868-Funk mit AES128-Bit-Verschlüsslung: Damit ist eine hohe Übertragungssicherheit gewährleistet, der bidirektionale Funk stellt sicher, dass das Funksignal angekommen ist
- Bis zu 1.000 m Funk-Reichweite (Freifeld)
- Jamming-Überwachung: Wird ein Störsender erkannt, schlägt Comfion Alarm
- Viele Möglichkeiten in einem System: 160 Geräte, 50 Benutzer, 40 Partitionen, 100 Szenarien
- Sicherheit für Ihren Kunden und die Versicherung: EN-Grad-2-Zertifizierung aller Alarmkomponenten
- Einen Sicherheitsdienst beauftragen: Leitstellenprotokoll integriert (SIA DC-09)
- Für Kommunikation & Zugriff: Integriertes Mobilfunkmodul (2G/3G/4G) für eine ausfallsichere Kommunikation, Alarmierung und Fernzugriff, auch ohne Internetanschluss am Standort
- Immer alle Informationen zur Hand: Benachrichtigungen wahlweise über SMS, E-Mail oder Push-Nachricht

2.2. Lieferumfang

		
1 x Zentrale	1 x Wandhalterung & 2 x Befestigungsschrauben	1x Akku
		
Kurzanleitung & Sicherheitshinweise	1 x Steckernetzteil	LAN-Kabel

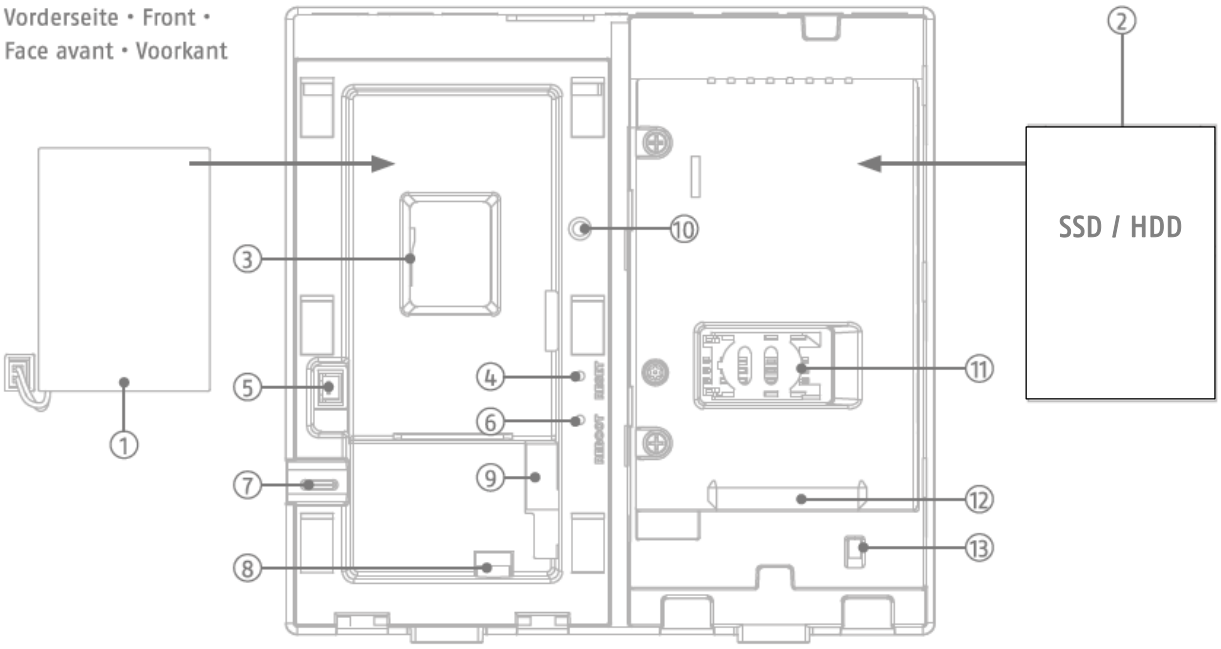
Benötigt:


2 x Schrauben / Dübel Ø 7.0 mm (M4)

2.3. Gerätebeschreibung

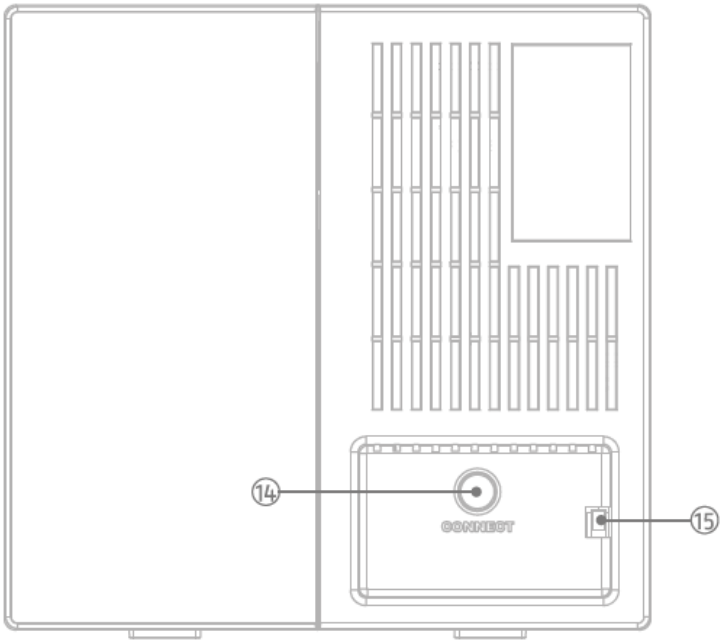
Produktaufbau

Vorderseite • Front •
Face avant • Voorkant



1. Notstrom-Akku	2. Festplatte (nicht im Lieferumfang)	3. MicroSD Karten-Schacht
4. Reset-Taste	5. Anschluss für Notstrom-Akku	6. Neustart-Taste
7. Kabeldurchführung	8. Anschluss externes Netzteil	9. RJ45-Buchse
10. Sabotageschalter (links)	11. SIM-Kartenschacht (Mini-SIM)	12. SATA-Festplattenanschluss
13. Sabotageschalter (rechts)	14. Taste Netzwerk-Rückstellung	15. Sabotageschalter (Wand)

Rückseite • Back •
Verso • Terug



Oberseite • Top •
En haut • Top

16. Power-LED
- Grün / Netzspannung
- Rot / Batteriebetrieb
- Gelb / Firmware-Update

18. Netzwerk-LED
- Grün / LAN
- Rot / 3G/4G-Mobilfunk

17. Internet-LED
- Grün / Online & Admin registriert
- Rot / offline
- Grün blinkend / online & Admin nicht registriert

19. Alarm-Status-LED
- Rot / Scharf
- Gelb / Teilscharf
- Grün / Unscharf
- Grün blinkend / Einlern-Vorgang Funk-Komponente

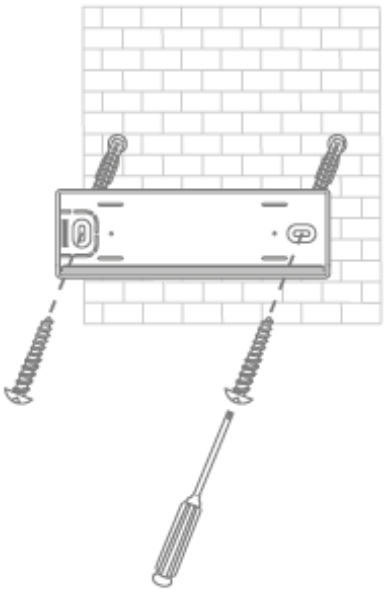
2.4. Technische Daten

Abmessungen (B x H x T)	165 x 165 x 61 mm
Gewicht	596g (mit Backup-Akku, ohne Festplatte)
Betriebstemperatur	-10 °C bis +40 °C
Umweltklasse	II (EN 50131-1 + A3:2020)
Luftfeuchtigkeit	max. 85% RH (Relative Luftfeuchte)
Anschlüsse	12V DC-Buchse, RJ45 (LAN), SATA-Anschluss, SIM-Kartenschacht, Micro-SD Kartenschacht
Anzeigen	Status LED (Power, Internet, Netzwerk, Systemstatus)
Tasten	Neustart-Taste, Reset-Taste
Funkfrequenz / Modulation	868.0 - 868.6 MHz / GFSK
Leistung, Funk / Reichweite	max. 25 mW (14dBm) / 1000m, Freifeld
Anzahl Funk-Komponenten	160
Anzahl Bereiche	40
Anzahl Benutzer	51
Anzahl Ereignisse	> 10.000
Kommunikation	Netzwerk-Schnittstelle: Ethernet 10/100 Mbps SSL/TLS Mobiles Netzwerk (Backup): 3G UMTS / 4G LTE SMS & Sprache: 2G GSM
Stromversorgung	Primär: DC-Netzteil 12V / 2A, Sekundär: LiPo-Akku 7,4V / 2.500mAh
Typ der Stromversorgung	Typ A, Spannungsversorgung konform gemäß EN50131-1+A3:2020 und EN50131-6+A1:2021
Pufferzeit - Batteriebetrieb	> 12 Std gemäß EN50131-1+A3:2020 Grad 2
Sabotagesicherheit (Erkennung / Schutz)	ja (1x Wandabriss-Kontakt; 2 x Gehäuse-kontakt)
Supervisionszeit	900 - 3.600 s (Voreinstellung: 3.600 s)
Sicherheitsgrad	Grad 2 (EN 50131-1 + A3:2020)
Konformität	Sicherheitsgrad 2 bei ordnungsgemäßer Installation konform gemäß EN 50131-1+A3:2020, EN 50131-3:2009 und EN 50131-5-3:2017
EU-Richtlinien	RED: 2014/53/EU, RoHS: 2011/65/EU + 2015/863 Allgemeine Sicherheit: 2001/95/EG

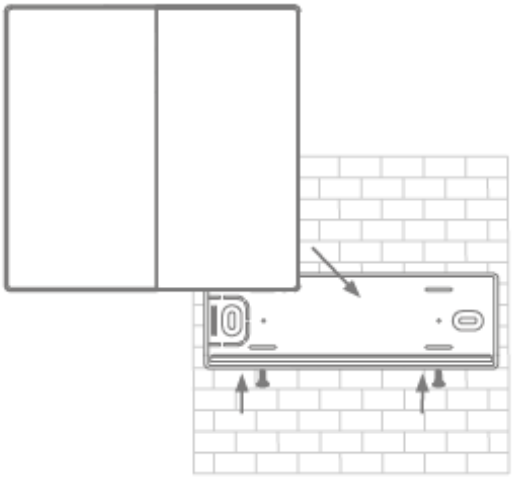
3. Montage & Inbetriebnahme

3.1. Wandmontage der Zentrale

Hinweis	- Montieren Sie die Zentrale auf ca. 1,5m Höhe an die Wand - Halten Sie zu allen Seiten einen Abstand von mindestens 1 m zu folgenden Geräten ein: Elektrogeräte, metallische Objekte oder Geräte mit Funkabstrahlung (z.B. Router, Mikrowellen) – da diese die Funk-Leistung des Systems beeinträchtigen können.



Befestigen Sie die Wandhalterung mithilfe von Schrauben & Dübel an die Wand. (z.B. M4 Halbrundkopf)



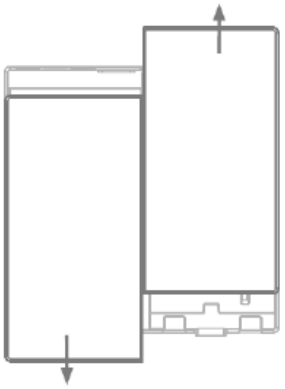
Platzieren Sie die Zentrale auf der Wandhalterung und fixieren diese mit den vormontierten Schrauben.

Hinweis	Das Entfernen der Zentrale von der Wandhalterung, sowie das Öffnen des Gehäusedeckels löst einen Sabotagealarm aus. Führen Sie notwendige Arbeiten an der Hardware nur dann aus, wenn der Wartungsmodus aktiviert ist (*Zentralen-Konfiguration –> Sicherheitseinstellungen*)

3.2. Inbetriebnahme des Systems

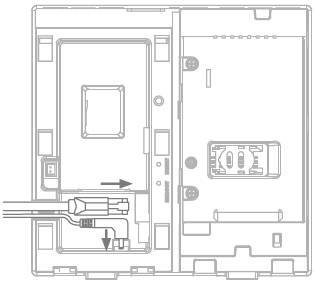
3.2.1. Vorbereitung der Hardware

- Schieben Sie die linke Abdeckung nach unten und die rechte Abdeckung nach oben, um das Gehäuse zu öffnen.



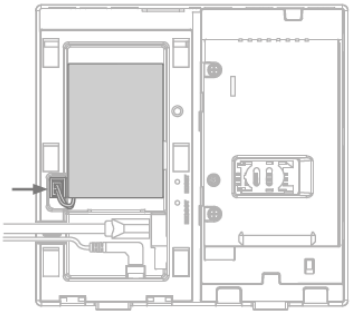
Hinweis	Wenn Sie eine Festplatte, SIM-Karte oder SD-Karte nutzen möchten, setzen Sie diese vor nächsten Punkt (Hinzugeben der Netzspannung) ein.

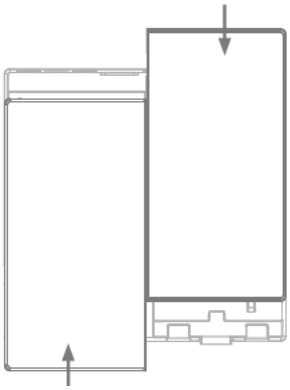
Hinweis	Formatieren Sie Ihre SD-Karte oder Festplatte vor dem Einlegen im Format exFAT oder NTFS. Während des Bootvorgangs der Zentrale darf nicht an der SD-Karte oder Festplatte gearbeitet werden.



- Schließen Sie das Ethernet-Kabel & Netzwerk-Kabel an der Zentrale an, um die Strom- und Netzwerkverbindung herzustellen und warten Sie, bis die 4 LEDs an der Zentrale aufleuchten (dies kann bis zu 40 Sekunden dauern).

- Schließen Sie den Notstrom-Akku an





- Schließen Sie das Gehäuse Mithilfe der beiden Frontabdeckungen

3.2.2. Einrichtung via App

Hinweis	Die Erstinbetriebnahme der Comfion-Zentrale und damit die Verknüpfung zum Fachpartnerportal und dem dazugehörigen Errichter muss per App stattfinden.

Schritt 1:
Laden Sie sich die Comfion-App aus Ihrem App-Store auf Ihr Mobilfunkgerät (IOS od. Android).

Schritt 2:
Folgen Sie den Anweisungen in der App bis Sie zur Login-Seite gelangen

Schritt 3:
Melden Sie sich mit ihren ABUS Single Sign-On Daten an (Partner-Zugang)
Falls Sie keinen Zugang besitzen, erstellen Sie sich ein (kostenloses) Konto unter dem Button „Registrieren".

Schritt 4:
Nach dem Login sehen Sie die Zentralenübersicht. Fügen Sie über den Plus-Button eine neue Zentrale hinzu.

Schritt 5:
Wählen Sie, wenn Sie die Anlage für einen Kunden in Betrieb nehmen „Ich bin ein Installateur". Hiermit werden Sie Rolle Installateur angelegt. Wenn Sie die Anlage für sich selbst installieren, wählen Sie „Ich bin ein Benutzer". Hiermit werden Sie als Rolle Admin mit Installateur & Adminrechten angelegt.

Schritt 6:
Scannen Sie den QR-Code auf der Rückseite der Zentrale.

Hinweis	Achten Sie darauf, dass die Anlage mit dem Internet verbunden ist.

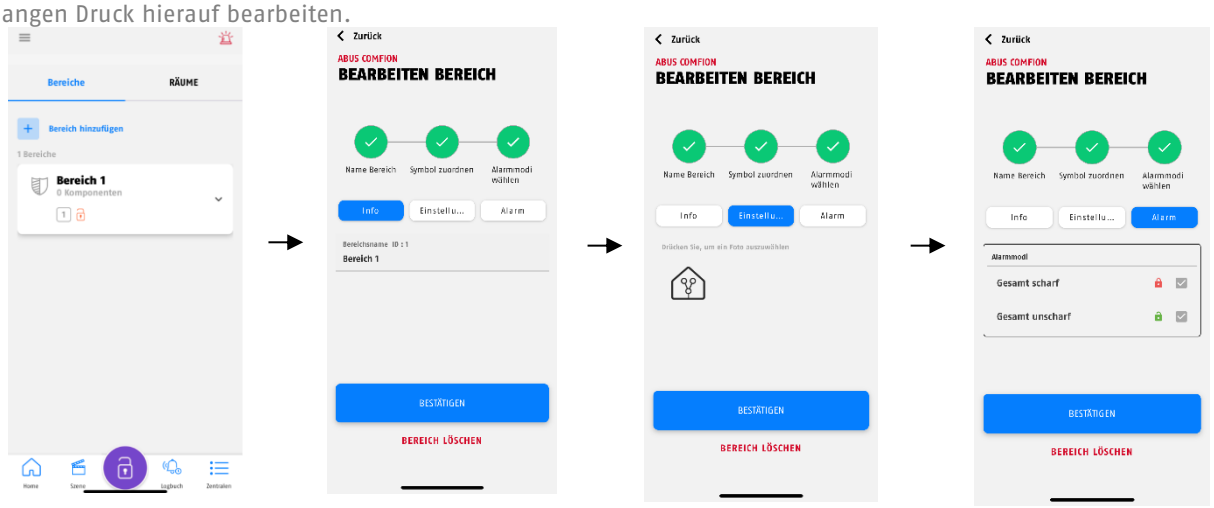
Schritt 7:
Vergeben Sie einen Zentralenname und bestätigen Sie diesen. Die Anlage wird nun ein Firmwareupdate starten, bevor Sie auf die Anlage zugreifen können. Das Firmwareupdate kann einige Minuten dauern und beinhaltet einen Neustart der Zentrale. Während des Updates blinkt die Power-LED Orange.

Schritt 8:
Nach dem Neustart der Zentrale ist die Anlage in der Zentralenübersicht nicht mehr ausgegraut und kann durch Klick hierauf aufgerufen werden.

3.2.3. Bereiche

Bereiche geben Ihnen die Möglichkeit, Ihr zu überwachendes Objekt aufzuteilen und somit auch differenziert scharf- und unscharf schalten zu können. Im Zusammenspiel mit den Alarmmodi können Sie Bereiche gemeinsam oder getrennt schalten.

Im Werkszustand verfügt die Anlage über einen vorkonfigurierten Bereich. Sie können diesen Bereich durch einen langen Druck hierauf bearbeiten.



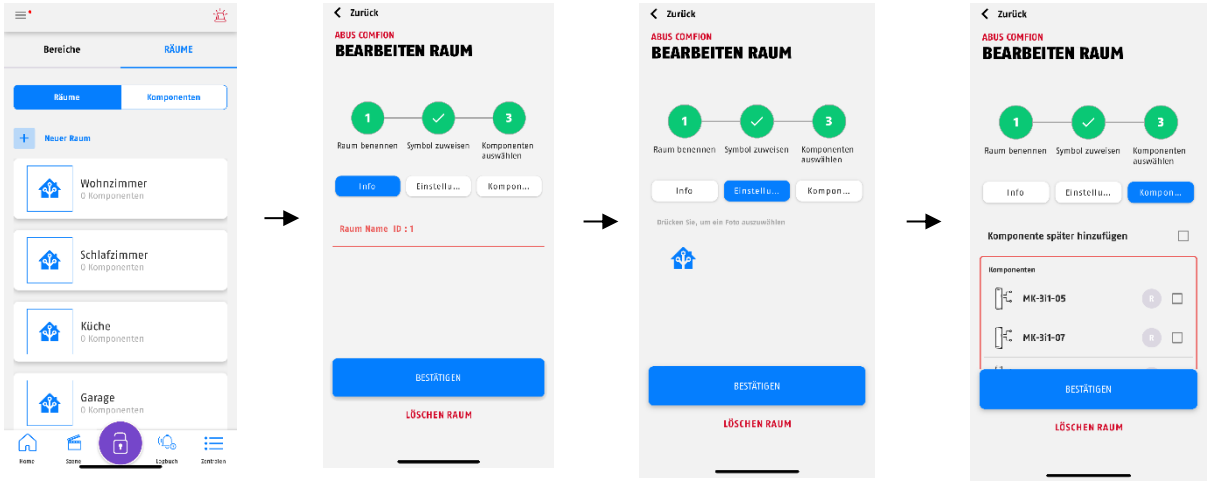
Durch Klick auf den Button „Bereich hinzufügen“ können Sie weitere Bereiche anlegen.

Bei dem Comfion Funk-Sicherheitssystem empfiehlt es sich, Außenhaut und Innenbereich in einzelne Bereiche aufzuteilen. Diese lassen sich dann durch die frei konfigurierbaren Alarmmodi beliebig scharf schalten.

3.2.4. Räume

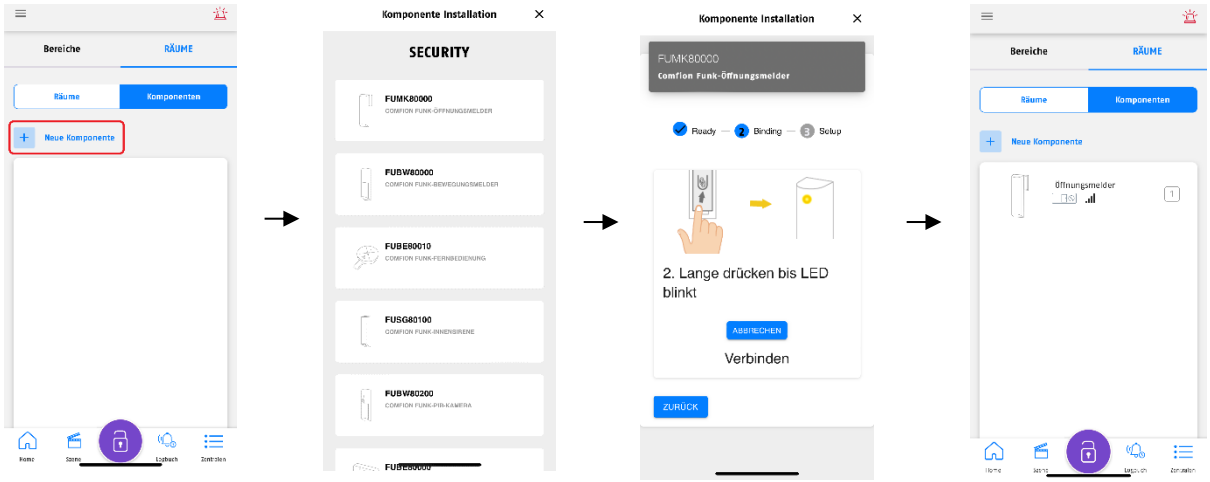
Das Comfion Funk-Sicherheitssystem bietet Ihnen die Möglichkeit, Ihre Komponenten Räumen zuzuweisen. Dies dient zur einfacheren Identifikation von Komponenten und hat keine funktionellen Eigenschaften. Räume sind keinen Bereichen zugeordnet, was bedeutet Sie können in einem Raum Komponenten aus verschiedenen Bereichen haben.

Im Werkszustand verfügt die Anlage über einige vordefinierte Räume. Sie können diese Räume frei bearbeiten, oder auch komplett löschen. Sie können diesen Bereich durch einen langen Druck hierauf bearbeiten.



3.2.5.Komponenten

Über den sich im Dashboard befindenden Reiter „Räume“ kommen Sie auf die Komponentenübersicht, bei welcher sich auch der Button „Neue Komponente“ befindet. Über diesen können Sie Ihre Comfion-Produkte dem System hinzufügen.



Durch einen langen Klick auf eine schon eingelernte Komponente können Sie diese außerdem bearbeiten und folgende Geräteeinstellungen anpassen:

Temporäre Deaktivierung	AUS (Default): Komponente normal in Funktion EIN: Komponente wird deaktiviert (keine Funktion)
Name	Namensvergabe der Komponente
Zonennummer	Vergabe der Zonennummer (geschieht automatisch durch System)
Zonentyp	• Eingang *-> löst eine Eingangsverzögerung aus, nach Ablauf wird ein Einbruchalarm ausgelöst* • Ausgang -> *kann während der Ausgangsverzögerung offen sein, funktioniert nach Scharfschaltung wie eine Sofort-Zone* • Eingang/Ausgang -> *nutzt eine Ein- & Ausgangsverzögerung* • Sofort (Einbruch) *-> löst bei scharfer Anlage einen Einbruchalarm aus* • Sofort (Überwacht) -> *funktioniert bei scharfer Anlage wie die Sofort-Zone; Bei unscharfer Anlage wird bei Auslösung eine Benachrichtigung versendet* • 24 Std. Einbruchalarm *-> Einbruchalarm unabhängig von Anlagenzustand* • 24 Std. Wasseralarm *-> Wasseralarm unabhängig von Anlagezustand* • 24 Std. Feuer *-> Feueralarm unabhängig von Anlagezustand* • Verschlussüberwachung -> *Offene Zone verhindert die Scharfschaltung, löst aber keinen Alarm aus*
Zonenverhalten	• Ausblendbar: *Wenn die Zone bei Scharfschaltung ausgelöst ist, haben Sie die Möglichkeit diese auszublenden* • Auslösung Sirene: *Dieser Melder steuert die in den Bereich integrierten Sirenen an* • Übertragungsbestätigung: *Wenn dieser Punkt aktiviert wird, wird die Meldung von Zonenalarmen um die Programmierte Zeit verzögert.*

Hinweis	Ist ein Melder auf den Zonentyp Ausgang oder Ein/Ausgang programmiert, prüft die Anlage bei Scharfschaltung den Melder-Status erst nach Ablauf der Verzögerungszeit. - Ist der Melder nach Ablauf der Zeit nicht bereit, und „Ausblendbar“ ist aktiviert, wird der Melder nach der Verzögerungszeit automatisch ausgeblendet und das System scharf geschaltet. - Ist der Melder nach Ablauf der Zeit nicht bereit, und „Ausblendbar“ ist deaktiviert, wird das System nicht scharf geschaltet.

s

3.2.6. Alarmmodi

Das Comfion Funk-Sicherheitssystem arbeitet mit sogenannten „Alarmmodi“, welche den Kern des Systems bilden. Es handelt sich hierbei um scharf- und unscharf- schaltbare Verknüpfungen zwischen Bereichen und Benutzern.

In einem Alarmmodus definieren Sie, welcher Benutzer welchen Bereich mit diesem scharf- oder unscharf schaltet. Hiermit lassen sich alle möglichen Szenarien der Scharf- und Unscharfschaltung abbilden.

In der Praxis führt ein Benutzer beim Scharf- oder Unscharf-schalten in Wirklichkeit einen Alarmmodus aus.

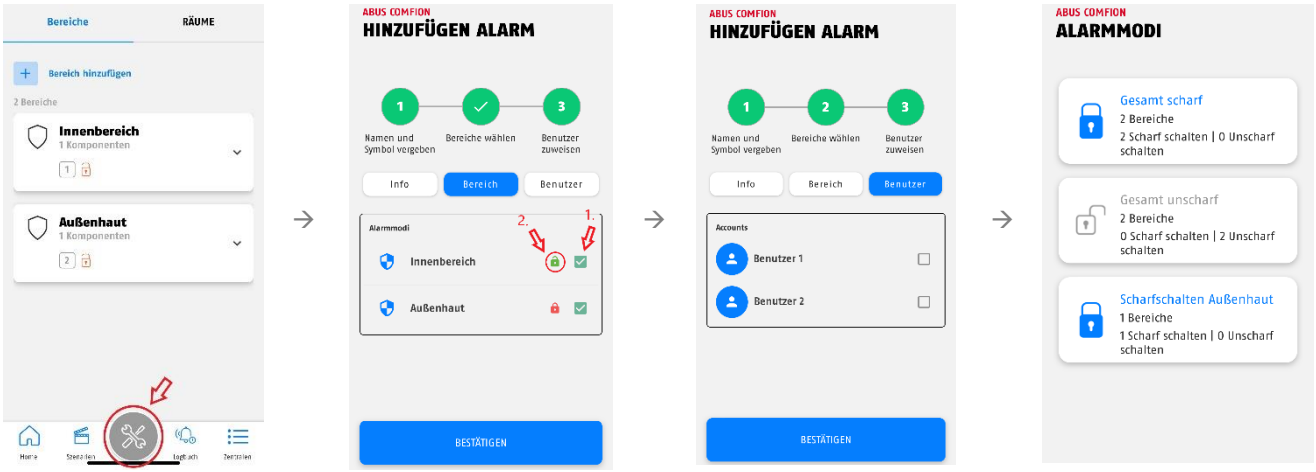
Hinweis	Das Comfion Funk-Sicherheitssystem hat im Werkszustand zwei vorkonfigurierte Alarmmodi: „Gesamt Scharf“ und „Gesamt unscharf“, welche alle erstellten Bereiche beinhalten.

Ausführung eines Alarmmodus

- Der im unteren Bildrand, mittige Button zeigt den aktuellen Status der Anlage (scharf, unscharf, teilscharf oder Wartungsmodus)
- Durch Drücken auf den Button werden Ihnen die vorhandenen Alarmmodi angezeigt und Sie können den beliebigen Schaltbefehlt ausführen.

Alarmmodi erstellen oder bearbeiten

1. Die Verwaltung der Alarmmodi können Sie öffnen, indem Sie wie im vorherigen Schritt beschrieben auf den unteren mittigen Button klicken und daraufhin auf das Einstellungssymbol im rechten oberen Bildrand.
2. Klicken Sie anschließend auf „Alarmmodus hinzufügen“ oder bearbeiten Sie einen bestehenden Alarmmodus durch langen Druck auf diesen.
3. Nachdem Sie den Namen für den Alarmmodus vergeben haben, wählen Sie die Bereiche UND die Art der Schaltung aus (Scharf od. Unscharf). Zum Ändern der Art der Schaltung, klicken Sie auf das Symbol.
4. Wählen Sie im nächsten Schritt die Benutzer, die die Berechtigung zur Schaltung dieses Alarmmodus haben sollen.
5. Nach Abschluss erscheint der Alarmmodus in Ihrer Übersicht und kann benutzt werden.



3.3. Kameras (NVR)

Mithilfe des Integrationsprotokolls ONFIV lassen sich diverse Kameras aus der ABUS Professional Line in das Comfion Funk-Sicherheitssystem einbinden. In die Comfion können Sie bis zu 4 Kameras einbinden und diese bei Event, bei scharfer Anlage oder dauerhaft (24/7) aufzeichnen lassen (SD oder SSD).

Hinweis	Zur Daueraufzeichnung wird eine Festplatte (SSD) in der Zentrale benötigt.

3.3.1. Einbinden von Kameras

Das Comfion-System sucht in der Werkseinstellung selbstständig nach ONFIV-Kameras im Netzwerk und fügt diese dem System hinzu. Die automatische Kamerasuche können Sie unter der Kameraübersicht in den Kamera Einstellungen deaktivieren.

Gehen Sie beim Einbinden der Kameras wie folgt vor:

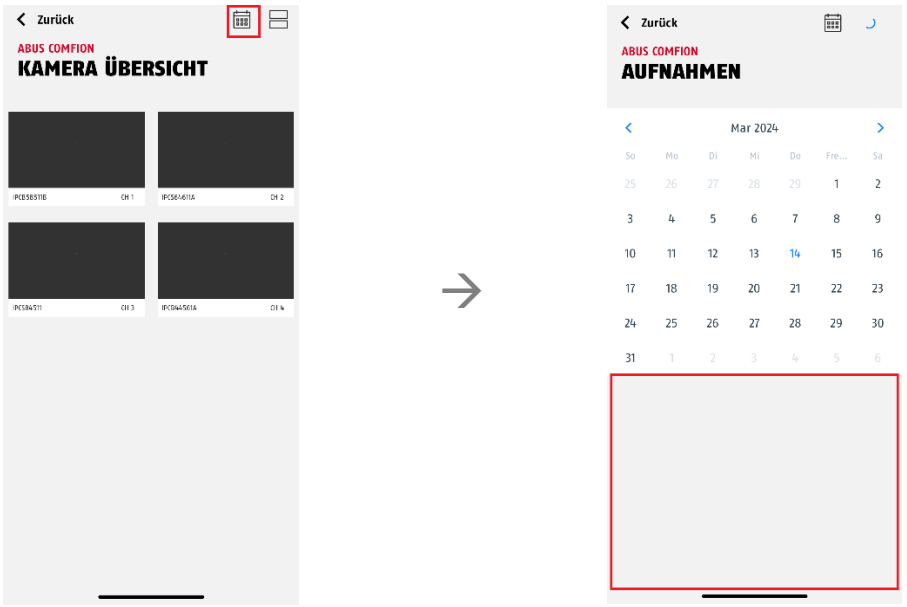
1. Binden Sie die Kamera in das gleiche Netzwerk wie die Comfion ein.
2. Öffnen Sie den ABUS IP-Installer und aktivieren die Kamera.
3. Öffnen Sie die Oberfläche der Kamera, loggen sich als Installateur ein und öffnen die Konfiguration.
4. Legen Sie unter den erweiterten Netzwerkeinstellungen unter Integrationsprotokoll ONVIF, speichern Sie diese Einstellung und legen Sie einen ONFIV-Benutzer an -> vergeben Sie den gleichen Benutzernamen und Passwort wie ein bestehender Admin oder Installateur an der Kamera. (Stellen Sie sicher, dass sie mindestens die ONFIV-Version 21.12 haben)
5. Nehmen Sie die im untenstehenden Hinweisfeld beschriebenen Video-Einstellungen in der Kamera vor
6. Hinterlegen Sie die ONFIV-Benutzerdaten in der Comfion
7. Testen Sie die Kamerafunktionen (Livebild, etc.)

Hinweis	Folgende Video-Stream-Einstellungen werden je nach Anzahl der eingebundenen Kameras (Kanäle) empfohlen, um auch bei gleichzeitigem Aufrufen und Daueraufzeichnen von 4 Kanälen einen störungsfreien Stream gewährleisten zu können. Primär-Stream: • 1 Kanal: Auflösung 1080p; Bitrate: 4096kbps • 2 Kanäle: Auflösung 1080p; Bitrate: 2048kbps • 3 Kanäle: Auflösung 1080p; Bitrate: 1024kbps • 4 Kanäle: Auflösung 1080p; Bitrate: 1024kbps Sekundär-Stream: • 1-4 Kanäle: Auflösung: 360p; Bitrate 512kbps

Hinweis	• Die maximale Auflösung von **4MP** je Kanal darf nicht überschritten werden • Die maximale Bitrate darf 4 x 2048kbps = 8192kbps zu keinem Zeitpunkt überschreiten (alle Kanäle addiert)

3.3.2. NVR-Bedienung

Über die Kamera-Übersicht gelangen Sie in die Parallelansicht, aller Kanäle. Sie können sich hier das Livebild aller eingebundenen Kameras anschauen. Über die kalender-Funktion können Sie sich die vorhandenen Aufnahmen im System nach Datum sortiert anschauen. Die Comfion schneidet die Aufnahmen in 15-minütige Clips.



Durch Klick auf den jeweiligen Kamera-Stream können Sie das Bild im Großformat anzeigen und erlangen Zugriff auf die spezifischen Funktionen der Kamera (z.B. PTZ, 2WayAudio, etc.).

4. Benutzer und Berechtigungsgruppen

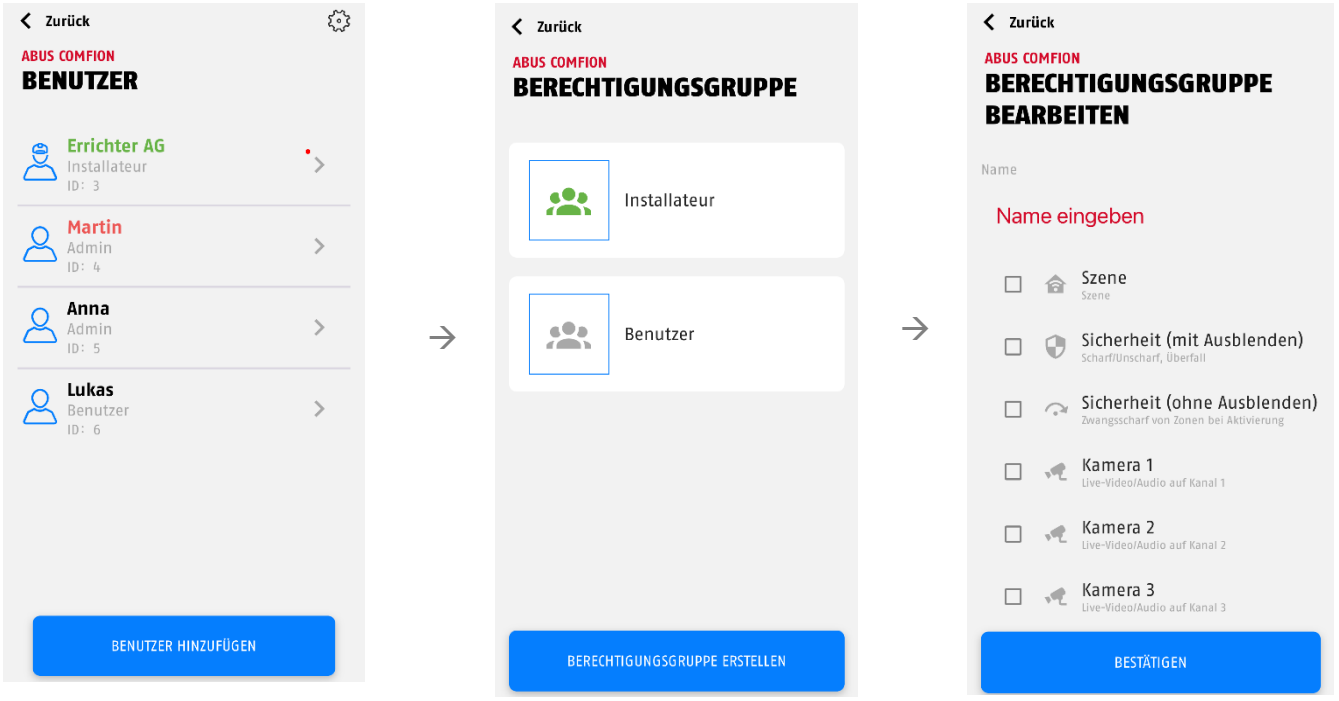
4.1. Erklärung der verschiedenen Rollen

Installateur	Der Installateur hat bei Erstinbetriebnahme alle Benutzerrechte. Nach der Übergabe der Anlage behält der Installateur alle Konfigurationsrechte. Der Besitzer der Anlage kann dem Installateur die Rechte für das Kamera-Livebild nehmen, und ihm den Zugriff auf die Anlage komplett sperren.
Admin	Der Admin der Anlage hat alle Benutzerrechte für die Anlage. Er kann außerdem Automationen und Szenen erstellen und bearbeiten. Der Installateur hat des Weiteren die Möglichkeit, den Admin mit Konfigurationsrechten auszustatten, sodass dieser die Rechte eines Installateurs bekommt.
Eigene Rolle (Benutzerdefiniert)	Sie haben die Möglichkeit eigene Nicht-Admin-Benutzergruppen zu erstellen und deren Berechtigungen festzulegen (Siehe unten)
Besitzer (Zusatzrolle)	Die Besitzer-Rolle wird automatisch dem ersten an der Anlage bestehenden Admin zugewiesen. Die Besitzer-Rolle kann nicht manuell vergeben werden. Der Besitzer der Anlage hat zusätzlich zu dem Admin-Rechten die Rechte Benutzer hinzuzufügen, einzuladen und zu löschen. Der Besitzer der Anlage ist in der Benutzerliste rot markiert.

Folgende Einstellungsmöglichkeiten gibt es unter dem Installateur-Benutzer:

- Zugriff freigeben: Sperrt/Gibt den Zugriff auf das System sowie Push-Benachrichtigungen
- Haupt-Installateur: Legt fest, mit welchen Installateur-Account die Anlage für die Fernwartung verbunden wird (Facherrichterportal)

Erstellen von Benutzergruppen:



4.2. Inbetriebnahme

Im Werkszustand der Zentrale gibt es aktuell die Berechtigungsgruppen „Installateur“ und „Admin“. Wenn die Anlage durch einen Installateur in Betrieb genommen wird, ist dieser zu Beginn für alle Funktionen in der Zentrale berechtigt.

4.2.1. Übergabe an den Besitzer

Nachdem Sie als Installateur die Einrichtung der Zentrale abgeschlossen haben, muss die Anlage an den Endnutzer übergeben werden. Der erste eingeladene Admin wird **der Besitzer** der Anlage. Dies erkennen Sie daran, dass dieser Nutzer rot markiert wird.
Nach dem Einladen des Besitzers verliert der Installateur die Rechte zum Bearbeiten und Hinzufügen von Nutzern. Weitere Nutzer müssen vom **Besitze**r hinzugefügt werden.

4.3. Einladen/Hinzufügen von Benutzern

Neue Benutzer können nach der Übergabe an den Besitzer nur durch diesen eingeladen werden. Zur Auswahl stehen beim Hinzufügen eines neuen Benutzers die folgenden Möglichkeiten:

- Neuen Benutzer einladen
  - Einladung eines Benutzers anhand der E-Mail-Adresse.
- Wählen von meinen Mitgliedern
  - Einladen eines Mitglieds. Mitglieder können in der Zentralenübersicht zu der persönlichen Mitgliederliste hinzugefügt werden. (Siehe **6.3.2 Mitglieder**)
- Lokalen Benutzer erstellen
  - Erstellen eines lokalen Benutzers ohne Abus Cloud Konto und ohne App-Nutzung. Dem lokalen Benutzer kann eine Fernbedienung und ein Code für das Bedienteil zugewiesen werden. Außerdem können Rufnummer & E-Mail für Benachrichtigungen hinterlegt werden.

Des Weiteren kann die Berechtigung des hinzuzufügenden Benutzers gewählt werden. Hierbei kann man zwischen Installateur, Admin und den selbst erstellten Benutzergruppen wählen.

4.4. Löschen von Benutzern

Es gibt zwei Möglichkeiten, Benutzer aus der Zentrale zu entfernen:

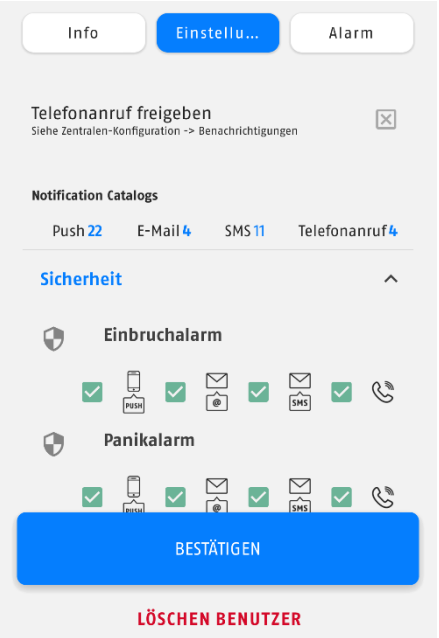
1. Der Besitzer der Anlage (rot markierter Benutzer) kann jeden anderen Benutzer durch Klick auf diesen und den Button „Benutzer löschen“ aus dem System entfernen.
2. Jeder Benutzer kann sich selbst aus der Anlage löschen, indem er in der Zentralenübersicht lange auf die betroffene Zentrale klickt und anschließend die Aufforderung zum Löschen bestätigt.

Hinweis	Der Besitzer der Anlage kann sich selbst nur durch den zweiten Weg (Zentrale aus Zentralenübersicht löschen) aus dem System entfernen. Nach dem Entfernen des Besitzers fällt die Rolle auf den Installateur zurück. Dieser kann durch Einladen eines neuen Admins diesen als neuen Besitzer kennzeichnen.

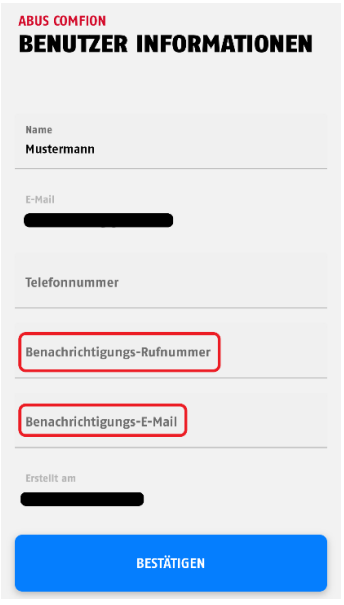
5. Kommunikation

Das Comfion Sicherheitssystem verfügt über folgende Kommunikationswege:
E-Mail, Push, SMS, Anruf & Leitstellenaufschaltung

Unter dem Menüpunkt „Benutzer“ können Sie bei jedem angelegten Benutzer einzeln wählen, welche Benachrichtigungen je Event versendet werden sollen.



Ihre Telefonnummer zur SMS & Telefonanruf, sowie Ihre E-Mail-Adresse für Benachrichtigungen werden in Ihrem Account hinterlegt. Sie können diese jederzeit ändern. Gehen Sie hierzu in Ihre Zentralenübersicht und klicken auf das Zahnrad in der rechten oberen Ecke. Nun können Sie die Benachrichtigungs-Rufnummer (**bitte mit Ländervorwahl, z.B. +49 eingeben**), sowie die Benachrichtigungs-E-Mail vergeben.



5.1. Mobilfunkmodul

Das Comfion Sicherheitssystem verfügt über ein integriertes Mobilfunkmodul (2G/3G/4G). Über dieses lassen sich SMS verschicken und Anrufe im Alarmfall tätigen. Es bietet außerdem einen Redundanzweg für die gesamte Kommunikation des Systems. Das heißt, dass bei Ausfall Ihrer Internetverbindung jegliche Kommunikation mit der Cloud, und somit auch der Fernzugriff sowie die Push-Benachrichtigungen über das Mobilfunkmodus abgehandelt werden.

Hinweis	Schalten Sie Ihre SIM-Karte vor dem Einlegen in das Mobilfunkmodul Pin-frei. Die PIN können Sie in der Regel in den Einstellungen eines beliebigen Handys abstellen.

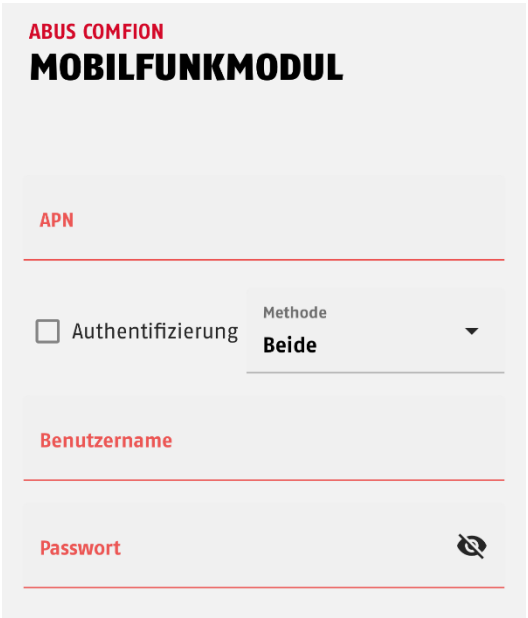
Hinweis	Verwenden Sie keine SIM-Karten aus dem Ausland für den Dauereinsatz in der Comfion.

Für den Betrieb des Mobilfunkmodus ist eine SIM-Karte notwendig. Diese SIM-Karte ist frei wählbar (Empfehlung ABUS: Telekom, Vodafone, o2) und muss über die Features verfügen, welche Sie an der Zentrale nutzen möchten. Wenn Sie alle Funktionen nutzen wollen, benötigen Sie eine SIM-Karte mit SMS, einen Sprachtarif sowie Datenvolumen.

Hinweis	ABUS rät aus Bedenken bzgl. der Verlässlichkeit davon ab, Prepaid-Karten im Comfion Sicherheitssystem zu nutzen. Des Weiteren ist ein Einsatz von Multi-SIMs nicht ratsam, da es zu Verbindungsproblemen führen kann.

RSSI-Wert	Bedeutung
-109 bis -95	Schlecht
-93 bis -85	Gering
-83 bis -75	Gut
-73 bis -53	Exzellent

Für den SMS-Versand sowie die Anruffunktion sind im Mobilfunkmodul selbst keine weiteren Einstellungen zu tätigen. Wenn Sie die Redundanz der Netzwerkdienste nutzen möchten, ist es notwendig die APN-Daten der eingesetzten Sim-Karte zu hinterlegen. Den Menüpunkt finden Sie unter „Zentralen-Konfiguration“ – „Mobilfunkmodul“.



Die APN-Daten Ihres Mobilfunkanbieters liegen Ihrer SIM-Karte bei. Alternativ können Sie diese online abfragen. Die Daten sind nicht SIM-Karten-spezifisch, sondern für jeden Anbieter gleich. Wenn bei den APN-Daten Benutzername & Passwort angegeben sind, setzen Sie den Haken bei „Authentifizierung“.

Beispiel Telekom:

- APN: internet.telekom
- Benutzername: t-mobile
- Passwort: tm

5.2. E-Mail

Der E-Mail-Versand der Comfion funktioniert ohne Konfiguration und wird über die Cloud abgehandelt.

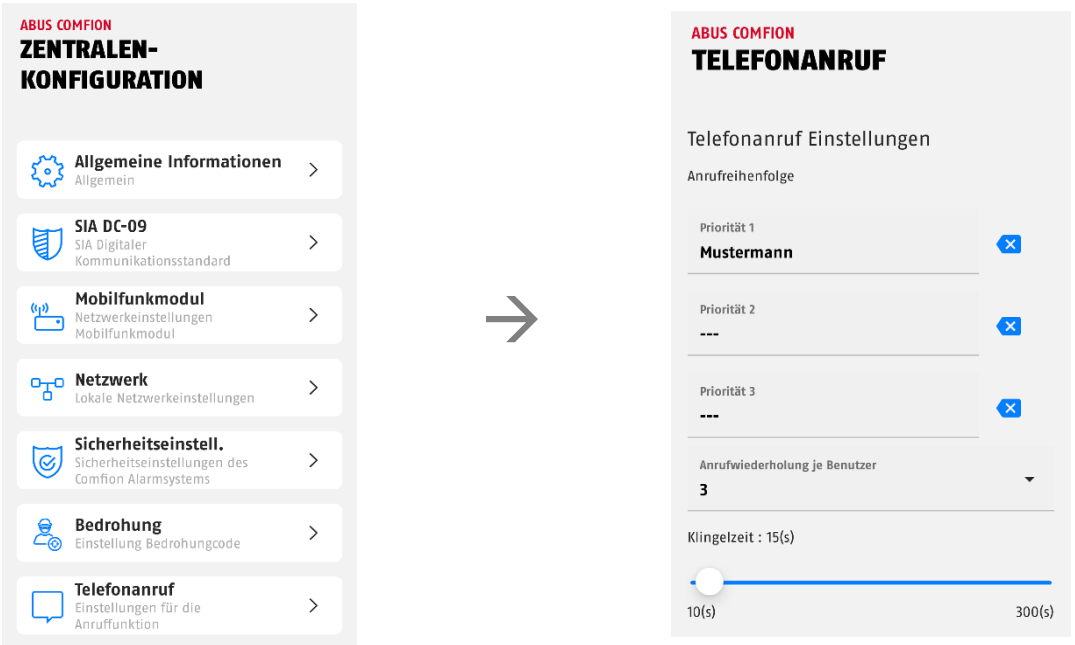
Falls die zu benachrichtigende E-Mail-Adresse von der Account-Mail abweichen soll, können Sie eine Benachrichtigungs-Adresse in Ihrem Account hinterlegen (siehe **5. Kommunikation**). Wenn Sie keine Benachrichtigungs-E-Mail hinterlegen, werden die E-Mails an Ihre Account-Adresse verschickt.

5.3. Telefonanruf

Das Comfion Sicherheitssystem kann Sie bei einem Alarm anrufen. Die Anlage verfügt über kein Sprachwählgerät, was bedeutet, dass keine Sprachnachricht bei diesem Anruf abgespielt wird. Der Anruf dient lediglich zur Alarmierung und soll helfen, den angerufenen Benutzer über einen Alarm zu informieren. Um was für einen Alarm sich handelt, kann der simultan versendeten Push-Benachrichtigung entnommen werden.

Für die Anruffunktion ist eine eingelegte SIM-Karte mit Anruffunktion und ausreichend Guthaben notwendig. Weitere Hinweise zum Mobilfunkmodul finden Sie unter **5.1 Mobilfunkmodul.**

- Um Anrufe zu erhalten, muss die Telefonnummer des Empfängers in dem Benutzerkonto hinterlegt werden (siehe **5**. Kommunikation).
- Des Weiteren müssen Sie unter „Zentralen-Konfiguration“ – „Telefonanruf“ die Anrufreihenfolge festlegen. Es können maximal 3 Benutzer hintereinander angerufen werden.



Hinweis	Die Anrufwiederholung je Benutzer ist werkstellig auf 3 gestellt. Das bedeutet, dass jeder Anrufer drei Anrufe bekommt. Der Anruf kann nicht bestätigt werden.

5.4. SMS

Das Comfion System kann SMS-Nachrichten anhand der Ereignisliste (Siehe **5. Kommunikation**) verschicken. Des Weiteren können Sie sich per Automationen SMS-Nachrichten mit frei definierbarem Text bei beliebigen Ereignissen schicken lassen.

Für die grundsätzliche Versandmöglichkeit von SMS muss lediglich eine SIM-Karte in das Modul eingelegt sein sowie die Benachrichtigungs-Rufnummer im Account hinterlegt sein (Siehe **5. Kommunikation)**.

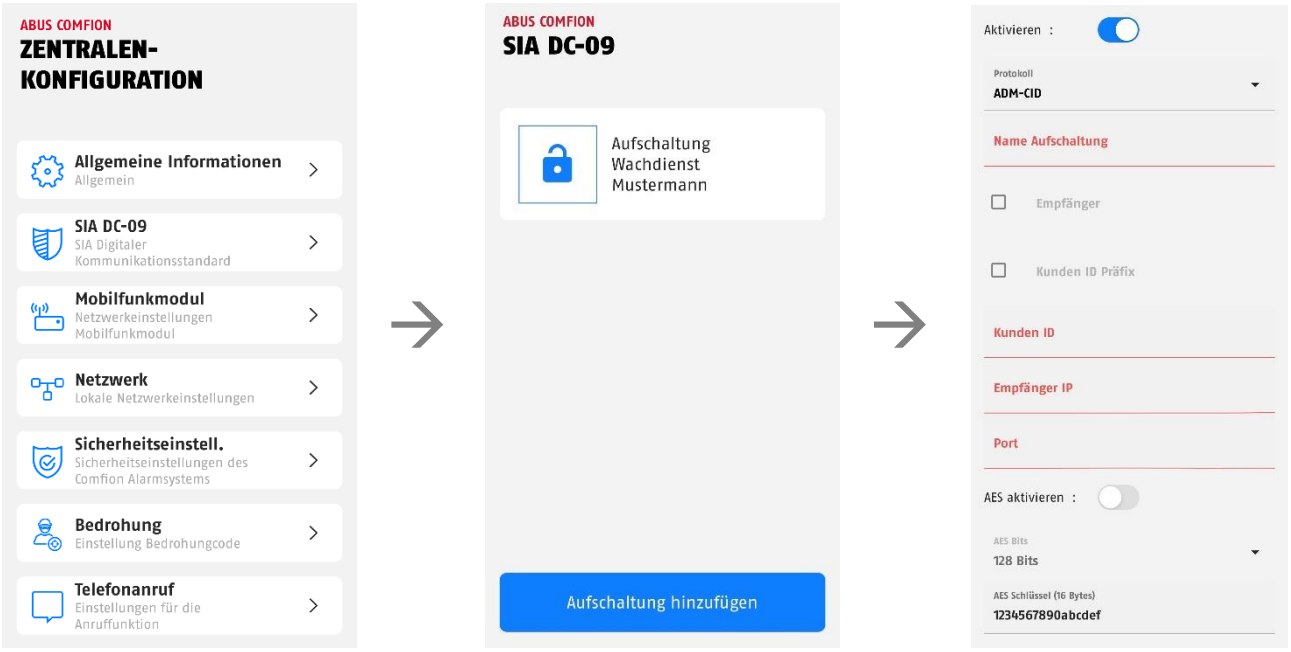
5.5. SIA DC-09 (Leitstellenaufschaltung)

Das Comfion Funk-Sicherheitssystem verfügt über ein digitales Leitstellenwählgerät welches das Protokoll Contact-ID über den Standard SIA DC-09 verschicken kann. Sie können mehrere Aufschaltungen gleichzeitig konfigurieren und somit an verschiedene Wachdienste kommunizieren.

Tragen Sie die von Ihrem Dienstleister erhaltenen Daten in die betroffenen Felder ein. Die beiden ausgegrauten Felder „Empfänger" sowie „Kunden ID Präfix" werden in der Regel nicht benötigt und müssen nur aktiviert werden, wenn es explizit von Ihrem Dienstleister gefordert wird.

Im Feld „Statische Testmeldung" können Sie zwischen folgenden Optionen wählen:

- **DC-09 Leitungsüberwachung** -> Im Leitstellenprotokoll integrierte Supervision (muss von Leitstelle unterstützt werden)
- **CID Testnachricht 602** -> Übertragung des Contact-ID Codes 602 im eingestellten Intervall



Über das Zahnrad-Symbol im rechten oberen Bildrand kommen Sie auf die Erweiterten Einstellungen.
In diesem können Sie die statische Testnachricht aktivieren, sowie den Intervall einstellen.

6. Allgemeines, Wartung und Hinweise

6.1. Zentralen-Konfiguration

Unter dem Menüpunkt Zentralen-Konfiguration finden Sie zum einen alle wichtigen Informationen zu Ihrer Zentrale und können des Weiteren wichtige Einstellungen zum System vornehmen

Nachdem Sie den Menüpunkt Zentralen-Konfiguration aufgerufen haben, sehen Sie als die folgenden Informationen:

- Zentrale Name (Eingabefeld)
- Symbol (Kann durch eigenes Foto ausgetauscht werden)
- Netzwerk (Anzeige der Art Netzwerkverbindung)
- Mobilfunkstatus (Drop-Down)
  - Modul Typ (verbauter Mobilfunkchip)
  - SIM-Karte (Anzeige ob eingelegt)
  - Telefonanruf (Anzeige ob mit eingelegter SIM möglich)
  - Verbindung (Anzeige über Verbindungsstatus)
  - Signalstärke (dBm)
- Stromversorgung (Anzeige Netzteil od. Akku)
- Firmware (Per Klick darauf Anzeige der Version u. der Release-Notes)
- Funkmodul (Anzeige der FW des Funkmoduls)
- Artikelnummer

Über das Zahnrad-Symbol rechts oben können Sie weitere Einstellungsmenüs öffnen. Die Einstellungen zu SIA DC-09, Telefonanruf und dem Mobilfunkmodul finden Sie unter 5. Kommunikation.

6.1.1. Allgemeine Informationen

Unter der Überschrift „Speicher“ werden die Ihnen Informationen zum eingelegten Speichermedium (Festplatte oder SD-Karte) angezeigt.

Unter der Überschrift „Datum und Uhrzeit“ werden Ihnen die verwendete Zeitzone sowie der NTP-Server angezeigt.

Mithilfe des Buttons „Neustart“ können sie die Anlage neustarten.

6.1.2. Netzwerk

In diesem Menü können Sie die Netzwerkeinstellungen einsehen und gegebenenfalls anpassen.

Sie haben drei mögliche Methoden als Auswahl:
DHCP (Default): Dynamic Host Configuration Protocol ist ein Client/Server-Protokoll, durch welches der Comfion automatisch seine IP-Adresse und andere zugehörige Informationen vom Router zur Verfügung gestellt werden.

PPPoE : Point-to-Point Protocol over Ethernet ist ein Netzwerk-Protokoll, welches die Direktverbindung im internen Netzwerk zur Verfügung stellt. Hierzu ist eine Authentifizierung per Benutzername und Passwort notwendig.

Statisch: Bei der Auswahl “statisch“ werden die Netzwerkdaten der Comfion manuell vergeben. Sprechen Sie dies mit dem Betreiber des Netzwerks ab und vergeben Sie keine IP-Adresse aus dem DHCP-Pool.

Hinweis	Falsche IP-Einstellungen führen dazu, dass Ihr System keine Verbindung zum Netzwerk herstellen kann, wodurch es für die App unerreichbar wird. Drücken Sie in diesem Fall die „connect“-Taste auf der Rückseite der Anlage für 6 Sekunden und lassen Sie sie dann los. Die Zentrale wird dann neu starten und ihre Netzwerkeinstellungen wieder auf die Standard-DHCP-Einstellungen zurücksetzen.

6.1.3. Sicherheitseinstellungen

Wartungsmodus	An/AUS (Default AUS)	Der Wartungsmodus dient zur Installation und Wartung des Systems. Während der Wartungsmodus aktiv ist, kann die Anlage keine Alarme auslösen.
Zonensperre	3x-20x (Default 5x)	Wenn eine Zone öfter ausgelöst wird als eingestellt, wird diese Zone nicht weiter auslösen, bis die Alarme aus dem Alarmverlauf gelöscht werden
Max. Wiederholung der Tastatureingabe	3x-20x (Default 5x)	Gibt an nach wie vielen falschen PIN-Eingaben am Bedienteil dieses gesperrt wird
Bedienteil-Timeout	5-180 sek (Default 30 sek)	Zeiteinstellung wie lange das Bedienteil nach X falschen Eingaben gesperrt ist
Eingangsverzögerung	5-45 sek (Default 10 sek)	Bei scharfer Anlage wird die Eingangsverzögerung durch eine Eingangs- oder Ein/Ausgangs-Zone ausgelöst
Ausgangsverzögerung	5-45 sek (Default 30 sek)	Zeit, bevor die Zentrale in den scharfen Zustand wechselt
Übertragungsverzögerung	5-180 sek (Default 60 sek)	Bei aktivierter Eigenschaft in der Zone wird die Übertragung einer Auslösung um die eingestellte Zeit verzögert.
Stromausfall Verzögerung	0-30 min (Default 0 min)	Einstellbare Verzögerung der Meldung eines Spannungsverlusts (12V DC)
Einbruch Sirene aktivieren	An/AUS (Default AN)	Sirenenansteuerung bei einem Einbruchalarm
Einbruchalarm Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Sabotage Sirene aktivieren	An/AUS (Default AN)	Sirenenansteuerung bei einem Sabotagealarm
Sabotagealarm Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Überfall Sirene aktivieren	An/AUS (Default AUS)	Sirenenansteuerung bei einem Überfallalarm
Überfallalarm Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Wasser Sirene aktivieren	An/AUS (Default AN)	Sirenenansteuerung bei einem Wasseralarm
Wasseralarm Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Feuer Sirene aktivieren	An/AUS (Default AN)	Sirenenansteuerung bei einem Feueralarm
Feueralarm Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Überfall APP Sirene aktivieren	An/AUS (Default AUS)	Sirenenansteuerung bei einem über die App ausgelösten Überfallalarm
Überfall APP Sirenendauer	5-180 sek (Default 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Ausblenden Netzwerkfehler	An/AUS (Default AUS)	Erkennung und Meldung eines Netzwerkfehlers
Ausblenden Akkufehler	An/AUS (Default AUS)	Erkennung und Meldung eines Akkufehlers
Ausblenden Stromverlust	An/AUS (Default AUS)	Erkennung und Meldung eines Stromverlusts (12V DC)
Ausblenden Deckelsabotage rechts	An/AUS (Default AUS)	Erkennung und Meldung einer Sabotage des rechten Deckels (Festplatte)
Ausblenden Deckelsabotage links	An/AUS (Default AUS)	Erkennung und Meldung einer Sabotage des linken Deckels (Akku)

6.1.4. Backup Zentrale

Hinweis	Die Backup-Datei Ihrer Zentrale wird aus Sicherheitsgründen vollverschlüsselt in der Abus Cloud, ausschließlich auf europäischen Servern, gespeichert.

Backup erstellen
Unter dem Menüpunkt Backup unter der Zentralen-Konfiguration können Sie manuell ein Backup erstellen sowie das automatische Backup aktivieren. Das automatische Backup wird wöchentlich durchgeführt.

Backup einspielen
Zum Importieren des Backups in eine neue Zentrale gehen Sie bitte wie folgt vor:

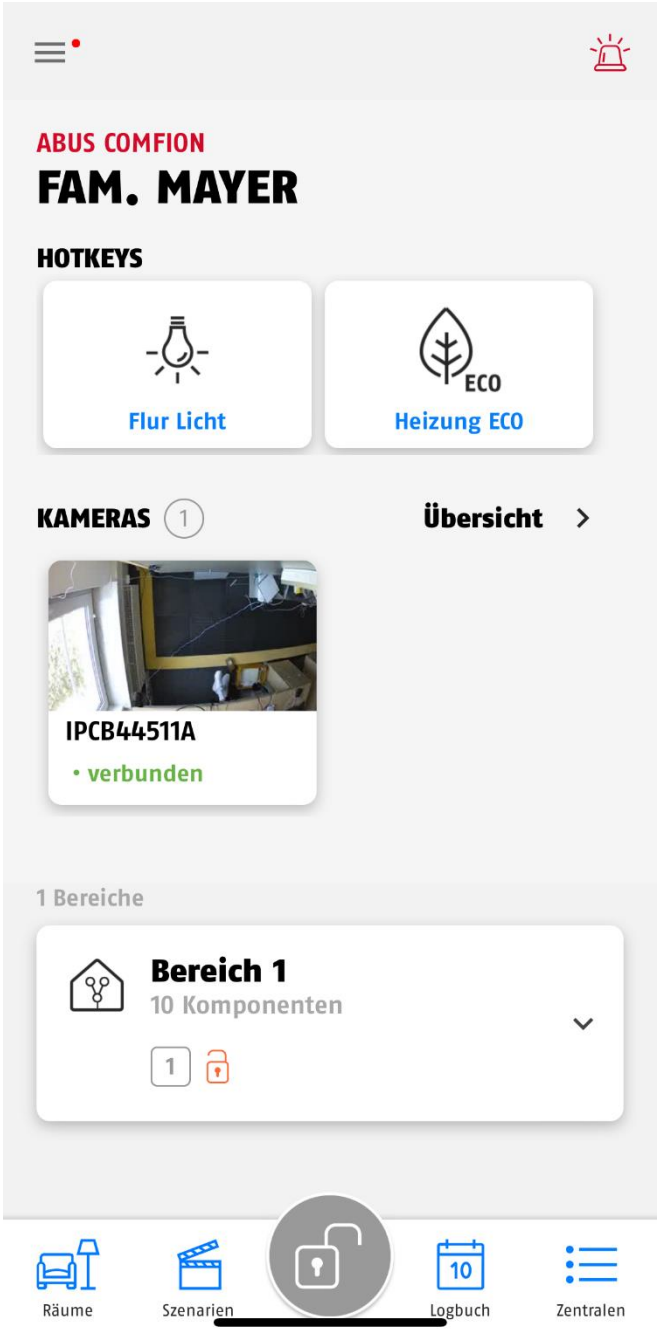
1. Trennen Sie Zentrale, von der das Backup stammt, falls noch nicht geschehen vom Netzwerk und schalten Sie sie ab.
2. Gehen Sie in der Zentralenübersicht in der App auf das + Symbol, um eine neue Zentrale hinzuzufügen
3. Wählen Sie „Backup Import“ aus
4. Scannen Sie den QR-Code auf der Rückseite Ihrer neuen Zentrale
5. Wählen Sie die Zentrale aus, von welcher Sie das Backup laden möchten
   Hinweis: Nach dem Importieren wird das Backup aus der Cloud gelöscht und die Komponenten funktionieren nicht mehr an der alten Zentrale.
6. Geben Sie den gewünschten Zentralennamen Ihrer neuen Zentrale ein
7. Nach dem Bestätigen wird ein Verifizierungscode an die E-Mail-Adresse des Besitzers der Anlage geschickt. Geben Sie diesen Code in der App ein und klicken Sie auf „Import starten“
8. Der Import wird nun durchgeführt. Sie können Ihre App nun schließen und warten, bis Sie die Push-Mitteilung erhalten, dass die Zentrale online und die Stromversorgung vorhanden ist.

Zum Wiederherstellen einer Konfiguration auf die gleiche Hardware (Zentrale) gehen Sie bitte wie folgt vor:

1. Setzen Sie die betroffene Zentrale auf Werkseinstellungen zurück (Reset-Button für 10 Sekunden betätigen -> siehe 6.5.1)
2. Gehen Sie in der Zentralenübersicht in der App auf das + Symbol, um eine neue Zentrale hinzuzufügen
3. Wählen Sie „Wiederherstellung“ aus
4. Scannen Sie den QR-Code auf der Rückseite Ihrer Zentrale
5. Geben Sie den gewünschten Zentralennamen Ihrer Zentrale ein
6. Der Import wird nun durchgeführt. Sie können Ihre App nun schließen und warten, bis Sie die Push-Mitteilung erhalten, dass die Zentrale online und die Stromversorgung vorhanden ist.

6.2. Dashboard

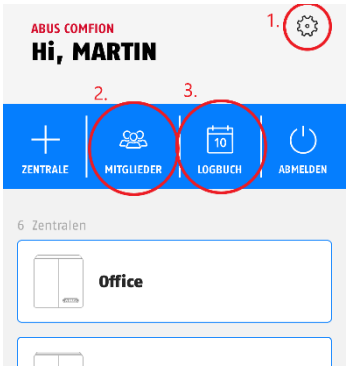
Über das Dashboard können Sie die Anlage steuern, und auch als Installateur einen Großteil Ihrer Arbeiten durchführen.



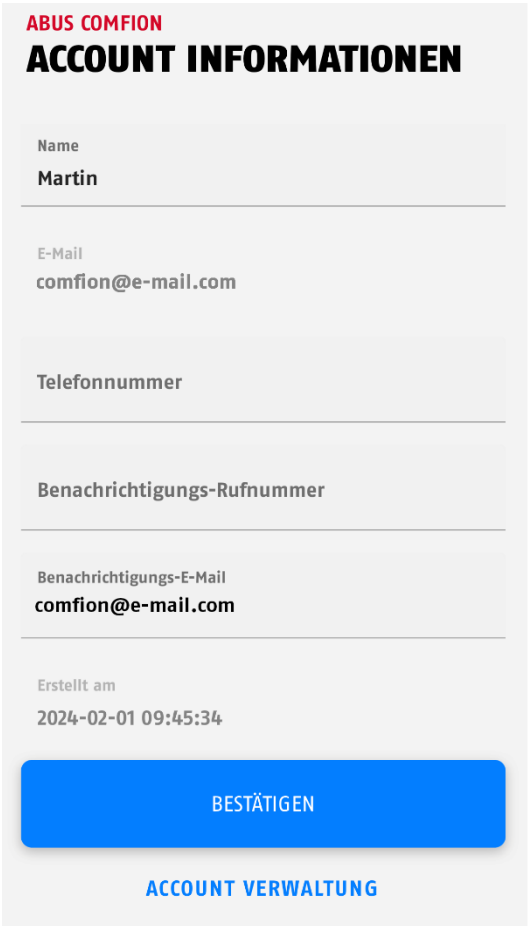
- Menüaufruf & Überfall-Taste
- Zentralenname
- Hotkeys – Können unter „Szenen“ festgelegt werden
- Kamera-Übersicht – Zugriff auf Kamera-Livestreams und Allgemeine Kameraeinstellungen
- Auswahl Kamera – Durch Klick auf die jeweilige Kamera wird direkt der Kamera-Livestream geöffnet
- Bereichsanzeige. Durch langen klick kann der Bereich bearbeitet werden. Durch kurzen klick wird der Bereich aufgeklappt und die zugewiesenen Komponenten angezeigt
- Räume = Anzeige der Raumübersicht & Komponenten
- Szenarien = Szenen & Automationen
- Logbuch = Anzeige des Ereignisspeichers
- Zentralen = Zentralenübersicht

6.3. Zentralenübersicht

In der Zentralenübersicht der Anlage können Sie neben dem Hinzufügen von neuen Zentralen die bestehenden Zentralen einsehen und darauf zugreifen, Ihre Account-Informationen bearbeiten (1), Ihre Mitglieder verwalten (2) und den Account-Log einsehen (3).



6.3.1. Account-Informationen



- ➔ Account Name (Anzeige in Zentrale & Logbuch)
- ➔ Account-E-Mail
- ➔ Telefonnummer
- ➔ Benachrichtigungs-Rufnummer für SMS & Anrufe
- ➔ Benachrichtigungs-E-Mail für E-Mail-Versand der Zentrale
- ➔ Erstellungszeitpunkt des Accounts
- ➔ Bestätigungsbutton zum Speichern der Eingaben
- ➔ In-App Lösch-Funktion des ABUS-Accounts

6.3.2. Mitglieder

In der Comfion-App haben Sie die Möglichkeit eine Mitgliederliste zu führen. Dies ist rein optional und wird zum Betrieb der Comfion Systeme nicht benötigt. Durch die Mitgliederliste können Sie beim Hinzufügen/Einladen von neuen Benutzern in einer Zentrale, diese ganz einfach aus Ihren Mitgliedern auswählen.

6.3.3. Account-Logbuch

Im Account-Logbuch werden alle Meldungen von zugriffsberechtigten Anlagen aufgeführt. Wenn der Zugriff auf eine Anlage gesperrt ist, werden Log-Einträge von dieser Zentrale nicht im Account-Log gespeichert.

6.4. Automationen & Szenen

Das Comfion System bietet ihnen die Möglichkeit bis zu 100 Szenarios zu konfigurieren. Diese Szenen oder Automationen können komplett frei eingestellt werden, was Ihnen eine maximale Flexibilität bietet.

Unter dem Reiter „Szenen“ können Sie sowohl Szenen als auch Automationen hinzufügen.

Achtung	Sich gegenseitig widersprechende oder zirkulär aufrufende Automationen dürfen nicht erstellt werden. Hierbei kann es zu schwerwiegenden Funktionsproblemen bei der Zentrale kommen.

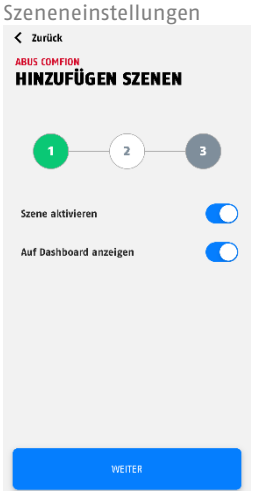
Hinweis	Achten Sie darauf, dass Sie zwischen zwei Schaltbefehlen für das gleiche Gerät einen Abstand von mindestens 5 Sekunden lassen, um einen reibungsfreien Betrieb sicherstellen zu können.

Szene = Aktion, welche durch einen User über die App getriggert wird (Hotkey). Kann im Dashboard angezeigt werden.
Beispiel: Steckdose AN/AUS über App

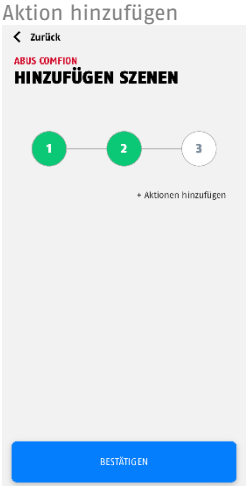
Beispielkonfiguration einer Szene:

Namens / Symbolvergabe

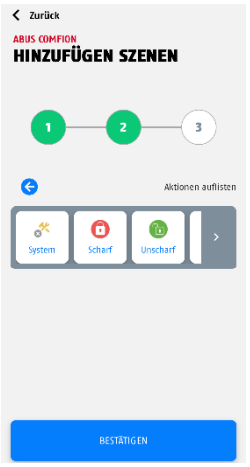
Szeneneinstellungen



Aktion hinzufügen



Auswahl Aktion



Automation = Besteht immer aus Wenn- und Dann-Teil. Frei konfigurierbar.
Beispiel: Wenn Anlage scharf, Dann Licht aus

Im Wenn-Teil kann zwischen einer Und-Verknüpfung & einer Oder-Verknüpfung gewählt werden. Bei der Und-Verknüpfung müssen ALLE Bedingungen erfüllt sein, dass die Aktion ausgeführt wird. Bei der Oder-Verknüpfung muss mindestens EINE Bedingung erfüllt sein, dass die Aktion ausgeführt wird.

Im Wenn-Teil kann bei den Ereignissen zwischen den folgenden Kategorien gewählt werden:

- System -> Hier finden Sie Systemereignisse wie ein Stromausfall, aber auch den Zeitplan
- Bereich -> Hier sind Bereichs-Ereignisse wie Scharf/Unscharf, Einbruch, Bereit zum Scharfschalten uvm. zu finden
- Zone -> Hier sind alle Zonen-Bezogenen Ereignisse zu finden (z.B. Zone Einbruch)
- Raum -> Hier sind alle Komponenten und die damit verbunden Ereignisse zu finden (z.B. Öffnungsmelder Kontakt geöffnet oder Wandtaster Taste gedrückt)

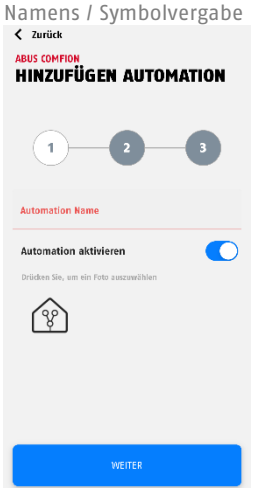
- Erklärung „Erweitert“:
  Unter „Erweitert“ kann eine Zeit eingestellt werden, welche definiert, wie lange die eingestellten Bedingungen zutreffen müssen, bis die Aktion ausgeführt wird. Nur wenn die Bedingungen für den Zeitraum der eingestellten Zeit zutreffen und sich nicht mehr verändern, wird die Aktion ausgeführt.
  Beispiel: Wenn Tür offen für 30 Sekunden, Dann Push-Benachrichtigung verschicken

Im Dann-Teil wird unterschieden zwischen

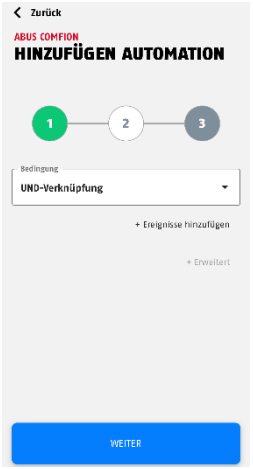
- „Wenn, dann“ -> Aktion wird ausgeführt, wenn die im Wenn-Teil bestimmten Bedingungen zutreffen
- „Wenn vorbei, dann“ -> Aktion wird ausgeführt, wenn die im Wenn-Teil bestimmten Bedingungen NICHT mehr zutreffen

Beispielkonfiguration einer Automation:

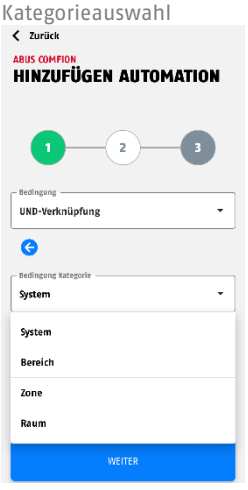
Namens / Symbolvergabe



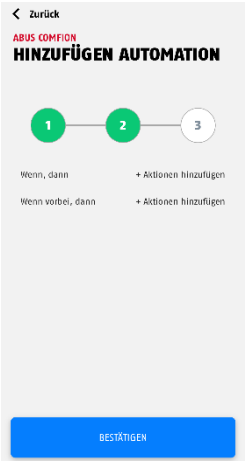
Wenn-Teil



Kategorieauswahl



Dann-Teil



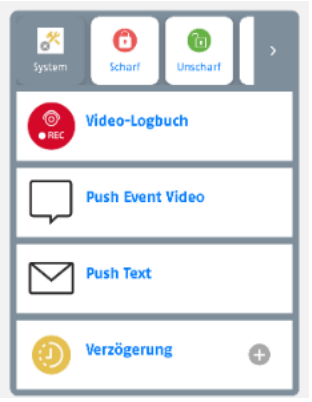
Bei der Auswahl „System“ im Dann-Teil von Szenen oder Automationen gibt es die folgenden Aktionsauswahlen:

Video Logbuch: Erstellen eines Logbucheintrags (15 Sek) mit Ausschnitt der Kameraaufnahme.

Push Event Video: Verschicken einer Push-Mitteilung mit definierbarem Text und Ausschnitt (15 Sek) aus der Kameraaufnahme.

Push Text: Verschicken einer Push-Mitteilung mit definierbarem Text.

Verzögerung: Einstellbare Verzögerung in Sekunden – z.B. zwischen zwei Aktionen



Bearbeiten einer Szene/Automation

Zum Bearbeiten halten Sie das Symbol der Szene/Automation für etwas 2 Sekunden gedrückt und lassen es wieder los

Löschen einer Szene/Automation

Sie können eine Szene/Automation löschen, indem Sie in den Bearbeitungsmodus gehen (siehe „Bearbeiten einer Szene/Automation) und anschließend auf den Button „Szene/Automation löschen“ im unteren Bildrand klicken.

6.5. Resets

6.5.1. Werksreset

Um die Anlage auf Werkseinstellungen zurückzusetzen, halten Sie die Reset-Taste (siehe *2.3 Gerätebeschreibung*) für >10 Sekunden gedrückt und lassen sie wieder los. Die LED's der Zentrale werden nach wenigen Sekunden aus gehen und die Anlage führt einen Neustart durch. Nach dem Neustart befindet sich die Zentrale auf Werkseinstellungen und kann neu eingerichtet werden.

6.5.2. User-Reset

Um die Benutzer der Anlage zurückzusetzen, bzw. alle Benutzer von der Anlage zu löschen, drücken Sie den linken Sabotagekontakt (oberhalb des Reset-Buttons) 5x innerhalb von 5 Sekunden. Nach einigen Sekunden geht die Internet-LED kurzzeitig auf Rot. Sie sollten auf den verbundenen Geräten eine Push-Mitteilung erhalten, dass die betroffene Zentrale entfernt wurde.

Wenn alle LED's wieder grün sind (Internet LED kann grün blinken), können Sie die Anlage über das +-Symbol in Ihrer App wieder neu hinzufügen.

6.5.3. Netzwerk-Reset

Falls Sie Ihre Anlage im Netzwerk aufgrund falscher IP-Einstellungen nicht mehr erreichen können, ist es möglich die Zentrale auf DHCP zurückzustellen. Halten Sie hierfür die Netzwerk-Rückstellung Taste auf der Rückseite der Zentrale (Beschrieben mit „Connect“) für 6 Sekunden gedrückt. Nach einigen Minuten sollte die Anlage wieder erreichbar sein.

6.6. Funktionsweise der LEDs

Hinweis	Die unten aufgeführten LED-Anzeigen gelten erst nach der Erstinbetriebnahme der Anlage

Power LED: Zeigt den Spannungszustand und kann Fehler signalisieren

Farbe	Bedeutung
Grün	Netzteilspannung
Rot	Akkubetrieb
Orange	Firmware Update

Internet LED (Globus): Zeigt den Status der Cloud-Verbindung

Farbe	Bedeutung
Grün	Mit Cloud verbunden (Besitzer ist angelegt)
Rot	Verbindung zur Cloud fehlgeschlagen
Grünes Blinken	Mit Cloud verbunden (Kein Besitzer angelegt)

Netzwerk LED (Pfeile): Zeigt den aktuell genutzten Kommunikationsweg

Farbe	Bedeutung
Grün	Per LAN mit dem Internet verbunden
Rot	3G/4G Verbindung

Status LED (Schloss): Zeigt Anlagenstatus

Farbe	Bedeutung
Rot	System Scharf
Orange	System Teilscharf
Grün	System Unscharf
Grünes Blinken	Zentrale verbindet sich mit Komponente

6.7. Bedienung

6.7.1. Scharf- / Unscharfschaltung

- APP: Die Scharf-/Unscharfschaltung kann in der App durch die Ausführung der Alarmmodi durchgeführt werden. Klicken Sie hierzu im Dashboard auf den mittigen Button im unteren Bildrand (Schloss-Symbol) und wählen Sie anschließend die Aktion aus (z.B. Gesamt scharf).
- BEDIENTEIL: Sie können das System über ein Funk-Bedienteil scharf- und unscharf schalten. Geben Sie hierzu Ihren Benutzercode ein und klicken anschließend auf die auszuführende Aktionsfläche (Schloss-Tasten). Genauere Informationen finden Sie im User-Guide oder in der Anleitung des Bedienteils
- FERNBEDIENUNG: Sie können die Tasten Ihrer Funk-Fernbedienung mit den Alarmmodi belegen und hiermit durch einen Tastendruck die jeweilige Aktion ausführen. Die Einstellung finden Sie unter der Fernbedienung.
- AUTOMATION: Über eine Automation können Sie die Scharfschaltung oder Unscharfschaltung der Anlage an Bedingungen knüpfen. Hiermit kann beispielsweise nach einem Zeitplan, oder beim Ansteuern eines Drahteingangs geschaltet werden.

6.7.2. Rückstellung von Alarmen

Das Comfion System muss nach einem Alarm (Einbruch, Sabotage, etc.) durch den Nutzer zurückgesetzt werden:

- Das Comfion System führt die Rückstellung des Alarms automatisch bei der Deaktivierung durch. Sobald sich alle ausgelösten Melder wieder im Normalzustand befinden, verschwindet die Warnungsübersicht aus dem Dashboard.

6.8. Symbolerklärung

	Komponente ausgelöst (z.B. Fenster geöffnet)
	Sabotage (z.B. Meldergehäuse geöffnet)
	Komponente angesteuert (z.B. Sirenenton ausgelöst)
	Komponentenstatus AUS (z.B. Funksteckdose aus)
	Komponentenstatus AN (z.B. Funksteckdose an)
	Bewegung erkannt
	PIR-Kamera: 1. Foto erstellen (Auslösetaste) 2. Aufnahme wird erstellt 3. Aufnahme wird übertragen
	Kabelbruch (z.B. 3in1 Melder)
	Spannungsversorgung angeschlossen
	Funkverbindung unterbrochen
	Zone geschlossen
	Zone geöffnet
	Ladezustand Batterie
	4 Balken = Exzellent 3 Balken = Sehr gut 2 Balken = Gut 1 Balken = OK 0 Balken = Schlecht

6.9. ABUS-Cloud

Das Comfion Funk-Sicherheitssystem verbindet sich bei der Erstinbetriebnahme mit der Abus Cloud. Die Anlage wird zudem im Abus Cloud Facherrichter-Account des Installateurs hinterlegt. Sollte dies nicht gewünscht sein, kann unter dem jeweiligen Benutzer in der Anlage der Haken bei „Haupt-Installateur“ entfernt werden, bzw. auch bei einem anderen Installateur gesetzt werden.

6.10. Hinweise zur Festplatte

- Die Schrauben zur Befestigung der Festplatte dürfen nur per Hand festgezogen werden
- Die Akkulaufzeit der Zentrale hängt unter anderem mit der verbauten Festplatte und deren Stromverbrauch, sowie der Anzahl der Kameras und der ausgewählten Aufzeichnungsart (Daueraufzeichnung, etc.) ab.
- Die in der Comfion verbaute Festplatte muss im Format exFAT oder NTFS formatiert sein
- Tauschen Sie die Festplatte nur im spannungslosen Zustand der Zentrale

6.11. Wartung und Instandhaltung durch Errichter

Testen Sie bei der routinemäßigen Wartung, dass das System ordnungsgemäß funktioniert:

- Überprüfen Sie die Comfion auf offensichtliche Anzeichen von Schäden an dem Gehäuse oder der Frontabdeckungen.
- Überprüfen Sie die Wirkung der Sabotageschalter (Wandabriss/Gehäusedeckel links, Gehäusedeckel rechts)
- Überprüfen Sie den Zustand der Notstrom-Akkus
- Reinigen Sie die das Gehäuse
    - Zum Reinigen wischen Sie bitte die Oberfläche mit einem trockenen, weichen Tuch ab.
    - Benutzen Sie kein Wasser, keine Lösungsmittel und keine Reinigungsmittel.
- Kontrollieren Sie die Signalstärke und den Batterie-/ Akkuzustand aller Komponenten
- Ersetzen Sie die Batterien bzw. Akkus wie in den Anweisungen des Herstellers empfohlen
- Testen Sie jede Komponente.
- Reinigen Sie vorsichtig die Linsen aller PIR-Melder und Kameras mit einem sauberen, trockenen, weichen Tuch.
    - Benutzen Sie kein Wasser, keine Lösungsmittel und keine Reinigungsmittel.
- Führen Sie einen Gehtest aller Melder durch.
- Testen Sie alle Signalgeber
- Testen Sie die Kommunikation.

Hinweis	ABUS empfiehlt einen Wechsel des Zentralen Akkus nach maximal 3 Jahren. Bei längerer Laufzeit kann ein plötzlicher Leistungsabfall nicht ausgeschlossen werden.

So wechseln Sie den Akku der Zentrale:

- Setzen Sie die Zentrale in den Wartungsmodus (Sicherheitseinstellungen)
- Öffnen Sie den linken Gehäusedeckel
- Trennen Sie die Spannungsversorgung sowie den alten Akku von der Zentrale
- Warten Sie 30 Sekunden
- Schließen Sie den neuen Akku sowie die Spanungsversorgung wieder an
- Schließen Sie den Deckel der Anlage und verlassen anschließend wieder den Wartungsmodus

6.12. Tabelle Funk-Signalstärken

Die folgende Tabelle beschreibt die Bedeutung der in dBm angezeigten Signalwerte der Comfion-Funk-Komponenten.

RSSI-Wert (dBm)	Bedeutung	Anzeige an Komponente
<= -100	Schlecht	0 Balken
<= -96	OK	1 Balken
<= -91	Gut	2 Balken
<= -86	Sehr gut	3 Balken
> -86	Exzellent	4 Balken

7. Release-Historie

7.1. Überblick

Datum der Veröffentlichung	Firmware-Version Zentrale	App Version IOS/Android
21.03.2024	1.0.4736	0.2.1360
26.03.2024	1.0.4751	Keine Änderung
10.05.2024	1.0.4957	0.3.1401
03.07.2024	1.0.5159	0.5.1471
16.09.2024	1.0.5398	0.5.1575 / 0.5.1577
11.11.2024	1.0.5500	0.6.1626
15.11.2024	1.0.5510	Keine Änderung
18.02.2025	1.0.5727	0.6.1702
28.02.2025	1.0.5782	Keine Änderung
18.03.2025	1.0.5836	Keine Änderung

7.2. Release Notes

Die Release-Notes zum aktuellen Firmwareupdate finden Sie in Ihrer Comfion App oder unter dem folgenden Link:
https://l.ead.me/becYdV

8. Gewährleistung

- ABUS-Produkte sind mit größter Sorgfalt konzipiert, hergestellt und nach geltenden Vorschriften geprüft.
- Die Gewährleistung erstreckt sich ausschließlich auf Mängel, die auf Material- oder Herstellungsfehler zum Verkaufszeitpunkt zurückzuführen sind. Falls nachweislich ein Material- oder Herstellungsfehler vorliegt, wird das Modul nach Ermessen des Gewährleistungsgebers repariert oder ersetzt.
- Die Gewährleistung endet in diesen Fällen mit dem Ablauf der ursprünglichen Gewährleistungszeit von 2 Jahren. Weitergehende Ansprüche sind ausdrücklich ausgeschlossen.
- ABUS haftet nicht für Mängel und Schäden, die durch äußere Einwirkungen (z.B. durch Transport, Gewalteinwirkung, Fehlbedienung), unsachgemäße Anwendung, normalen Verschleiß oder durch Nichtbeachtung dieser Anleitung sowie der Pflege-Hinweise entstanden sind.
- Bei Geltendmachung eines Gewährleistungsanspruches ist dem zu beanstandenden Produkt der originale Kaufbeleg mit Kaufdatum und eine kurze schriftliche Fehlerbeschreibung beizufügen.
- Sollten Sie an dem Produkt einen Mangel feststellen, der beim Verkauf bereits vorhanden war, wenden Sie sich innerhalb der ersten zwei Jahre bitte direkt an Ihren Verkäufer.

9. Entsorgungshinweise

Entsorgen Sie das Gerät gemäß der Elektro- und Elektronik-Altgeräte EU Richtlinie 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). Bei Rückfragen wenden Sie sich an die für die Entsorgung zuständige kommunale Behörde. Informationen zu Rücknahmestellen für Ihre Altgeräte erhalten Sie z.B. bei der örtlichen Gemeinde- bzw. Stadtverwaltung, den örtlichen Müllentsorgungsunternehmen oder bei Ihrem Händler.

10. Konformität

10.1. EU-Konformitätserklärung

Hiermit erklärt ABUS Security Center GmbH & Co. KG dass der Funkanlagentyp FUAA80000 der Richtlinie 2014/53/EU und 2011/65/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: abus.com > Artikelsuche > FUAA80000 > Downloads

10.2. Konformität nach EN 50131

Das Sicherheitssystem FUAA80000 ist zertifiziert nach Sicherheitsgrad 2 bei ordnungsgemäßer Installation konform gemäß EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 und EN 50131-5-3:2017.

ABUS I Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel: +49 82 07 959 90-0

ABUS
Security Tech Germany

FUAA80000

INSTALLER MANUAL

Comfion wireless security system

V2.0

1. General

1.1. Introduction

Thank you for choosing the **Comfion wireless security system**, a product from ABUS Security Center (also known as "ABUS" for short).

This manual contains important descriptions, technical data, overviews and further information on project planning, start-up and operation of the **Comfion wireless security system**.

The products/systems described here may only be installed and maintained by persons who are qualified for the respective task. Qualified personnel for installation and maintenance of the system are usually trained ABUS specialist partners.

1.2. Intended use / Legal information

The responsibility for the legally compliant use of the product lies with the purchaser or customer and the end user. In accordance with the manufacturer's liability for its products as defined in the Product Liability Act, the above information must be observed and passed on to operators and users. Non-compliance releases ABUS Security Center from legal liability.

Use for other than the agreed purpose or unusual use, repair work or modifications not expressly authorised by ABUS, and improper servicing can lead to malfunctions and must be avoided. Any modifications not expressly authorised by ABUS will result in the loss of liability, warranty and separately agreed guarantee claims.

Architects, technical building planners (technical building services) and other consulting institutions are required to obtain all necessary product information from ABUS in order to fulfil the information and instruction obligations in accordance with the Product Liability Act. Specialist dealers and installers are required to observe the information in the ABUS documentation and to pass it on to their customers if necessary.

Further information can be found at www.abus.com on the general page, or for dealers and installers in the partner portal at https://partner-asc.abus.com/

1.3. Customer Service / Customer Support

For further assistance, please contact our support team: support@abus-sc.com

General information on the **Comfion wireless security system** can be found on our homepage at:
https://www.abus.com/int/Consumer/Alarm-systems/Comfion-wireless-system

1.4. Publisher information

Edition English 0/2024

This edition loses its validity with the publication of newer installation instructions.

ABUS Security Center accepts no liability for technical or typographical errors and their consequences. The information in these installation instructions has been compiled to the best of our knowledge and belief, taking into account the current state of the art. It is regularly reviewed and updated or corrected as necessary.

All trademarks and industrial property rights are recognised, changes in the sense of technical progress can be made without prior notice.

1.5. Explanation of symbols

The following symbols are used in these installation instructions:

Symbol	Signal word	Meaning
	Caution	Indicates a risk of injury or health hazard due to electrical voltage
	Important	Indicates possible damage to the device/accessories or a risk of injury or health hazards
	Note	Indicates important information

2. Functional principle and features

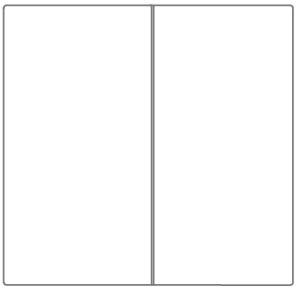
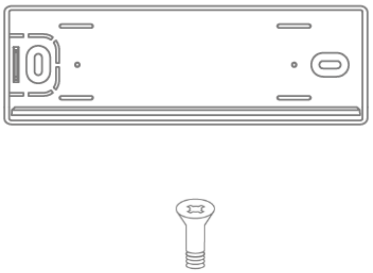
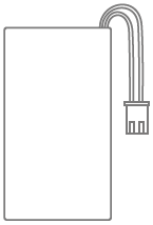
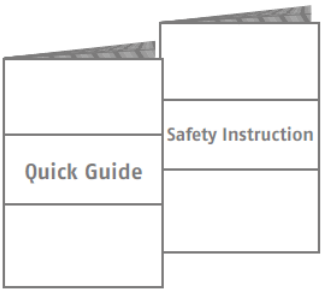
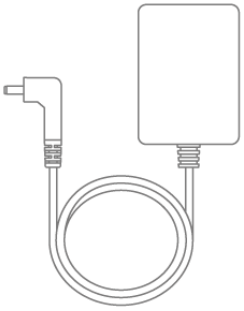
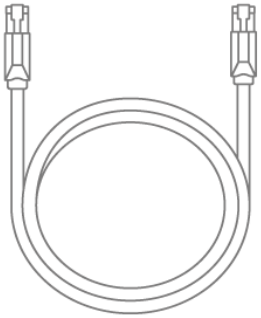
2.1. Product features

The **FUAA80000 Comfion wireless security system** is an EN Grade 2-certified security system with smart home functions. The system can be set up and operated via the intuitive app or the ABUS Cloud Portal.

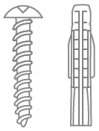
Main features:

- Simple installation: retrofitting is possible at any time with little effort thanks to wireless technology
- Integrated NVR: Video recording with up to 4 cameras on SD card or 4-channel NVR directly in the control panel, deep integration of ABUS Professional Line cameras
- Secure 868 radio transmission with AES128-bit encryption: this ensures a high level of transmission security, while the bidirectional radio ensures that the radio signal has arrived
- Up to 1,000 m radio range (free field)
- Jamming monitoring: if a jammer is detected, Comfion issues an alert
- Many possibilities in one system: 160 devices, 50 users, 40 partitions, 100 scenarios
- Security for your customer and the insurance company: EN Grade 2 certification of all alarm components
- Use of a security service: integrated control centre protocol (SIA DC-09)
- For communication & access: integrated modem (2G/3G/4G) for fail-safe communication, alerting and remote access, even without an internet connection on site
- All information always at hand: notifications optionally via text message, e-mail or push message

2.2. Scope of delivery

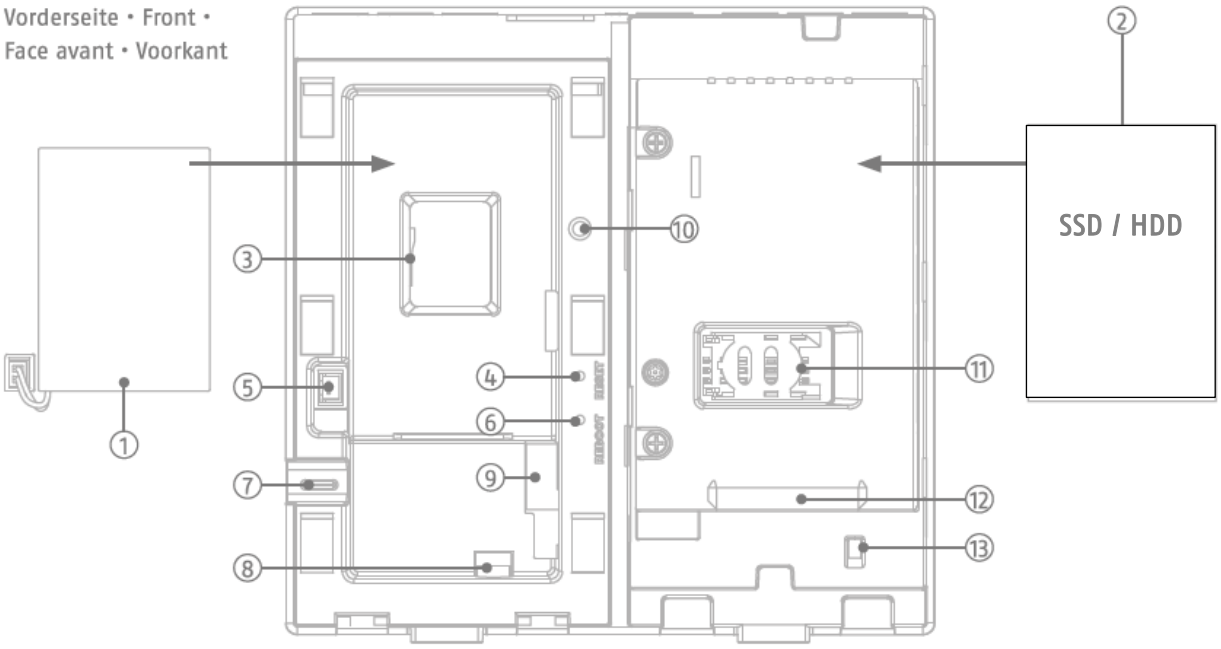
		
1 x control panel	1 x wall bracket 2 x mounting screws	1x battery
		
Quick guide & safety information	1 x plug-in power supply	LAN cable

Required:


2 x Screws / Plugs Ø 7.0 mm (M4)

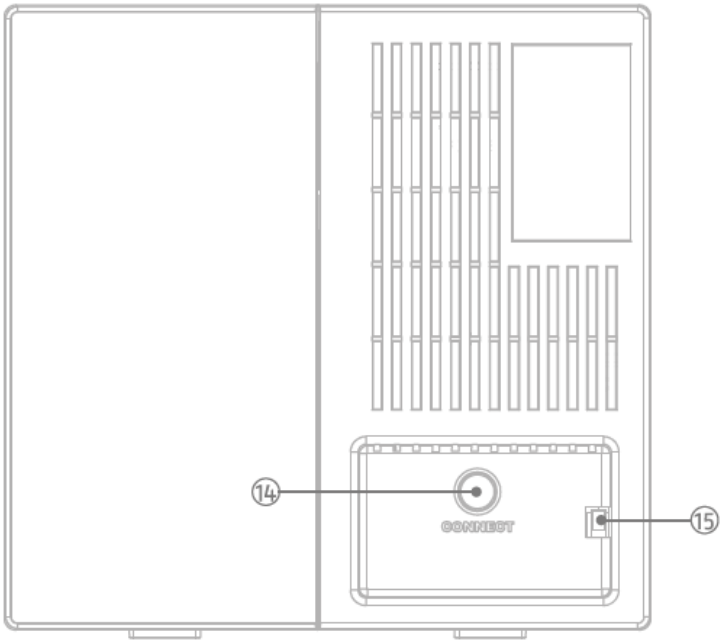
2.3. Device description

Product structure

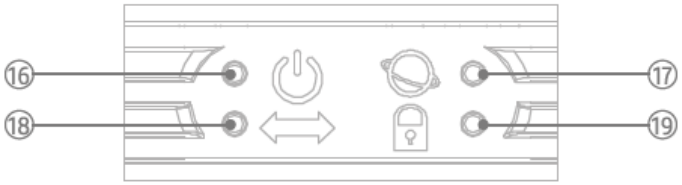


1. Backup battery	2. Hard drive (not included)	3. MicroSD card slot
4. Reset button	5. Connection for backup battery	6. Restart button
7. Cable bushing	8. External power supply connection	9. RJ45 socket
10. Tamper switch (left)	11. SIM card slot (mini SIM)	12. SATA hard drive connection
13. Tamper switch (right)	14. Network reset button	15. Tamper switch (wall)

Rückseite • Back •
Verso • Terug



Oberseite • Top •
En haut • Top



16. Power-LED
- Green / Mains voltage
- Red / battery operation
- Yellow / firmware update

18. Network-LED
- Green / LAN
- Red / 3G/4G mobile radio

17. Internet-LED
- Green / Online & Admin registered
- Red / offline
- Flashing green / online & admin not registered

19. Status-LED
- Red / Armed
- Yellow / Partially Armed
- Green / Disarmed
- Flashing green / Pairing process Radio component

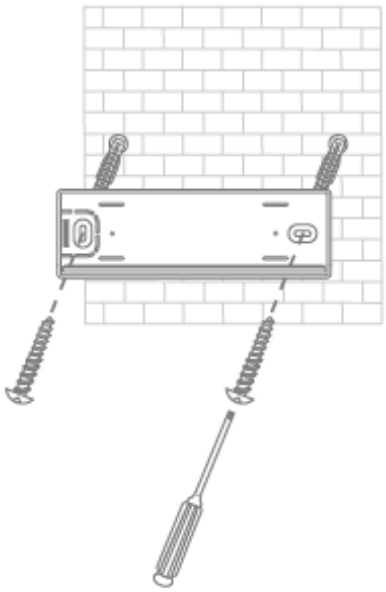
2.4. Technical data

Dimensions (W x H x D)	165 x 165 x 61 mm
Weight	596 g (with backup battery, without hard drive)
Operating temperature	-10°C to 40°C
Environmental class	II (EN 50131-1 + A3:2020)
Humidity	max. 85% RH (relative humidity)
Connections	12 V DC socket, RJ45 (LAN), SATA connection, SIM card slot, MicroSD card slot
Displays	Status LED (power, internet, network, system status)
Buttons	Restart button, reset button
Radio frequency / modulation	868.0 - 868.6 MHz / GFSK
Power, radio / range	max. 25 mW (14 dBm) / 1000 m, free field
Number of wireless components	160
Number of partitions	40
Number of users	51
Number of events	> 10.000
Communication	Network interface: Ethernet 10/100 Mbps SSL/TLS Mobile network (backup): 3G UMTS / 4G LTE text message & voice: 2G GSM
Power supply	Primary: DC power supply unit 9 V / 2 A, secondary: LiPo battery 7.4 V / 2,500 mAh
Type of power supply	Type A, power supply compliant with EN50131-1+A3:2020 and EN50131-6+A1:2021
Buffer time – battery operation	> 12 hours according to EN50131-1+A3:2020 Grade 2
Tamper protection (detection/protection)	yes (1x wall tear-off contact; 2 x housing contact)
Supervision time	900 - 3,600 s (default setting: 3,600 s)
Security level	Grade 2 (EN 50131-1 + A3:2020)
Conformity	Security grade 2 with proper installation compliant with EN 50131-1+A3:2020, EN 50131-3:2009 and EN 50131-5-3:2017
EU Directives	RED: 2014/53/EU, RoHS: 2011/65/EU + 2015/863 General safety: 2001/95/EC

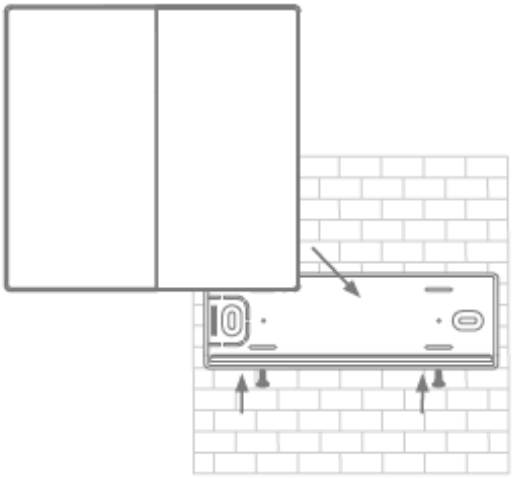
3. Installation and start-up

3.1. Wall mounting of the control panel

Note	- Install the control panel on the wall at a height of approx. 1.5 m - Maintain a distance of at least 1 m from the following devices on all sides: Electrical appliances, metal objects or devices with radio emissions (e.g. routers, microwaves) as these can impair the wireless performance of the system.



Attach the wall bracket to the wall using the screws and wall plugs supplied. (e.g. using M4 semi-round head screws)



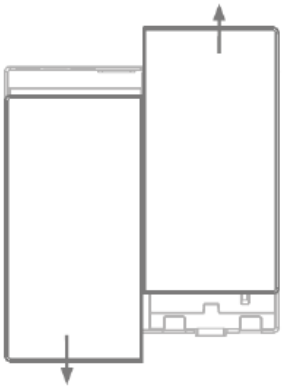
Place the control panel on the wall bracket and secure it with the pre-assembled screws.

Note	Removal of the control panel from the wall bracket and opening the housing cover will trigger a tamper alarm. Only carry out necessary work on the hardware when maintenance mode is activated *(Gateway configuration -> Alarm*)

3.2. Putting the system into operation

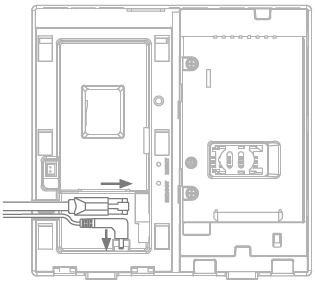
3.2.1. Preparing the hardware

- Slide the left cover downwards and the right cover upwards to open the housing.

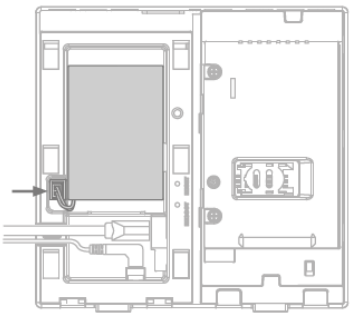


Note	If you want to use a hard drive, SIM card or SD card, insert it before the next step (adding the mains voltage).

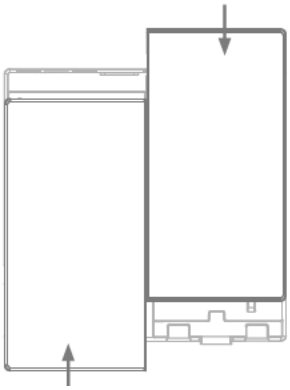
Note	Format your SD card or hard drive in exFAT or NTFS format before inserting it. Never work on the SD card or hard drive while the control panel is booting.



- Connect the Ethernet cable & network cable to the control panel to establish the power and network connection and wait until the 4 LEDs on the control panel light up (this can take up to 40 seconds).



- Connect the emergency power battery



- Close the housing using the two front covers

3.2.2. Setup via app

Note	The initial start-up of the Comfion control panel and thus the link to the specialist partner portal and the associated installer must take place via app.

Step 1:
Download the Comfion app from your app store onto your mobile device (IOS or Android).

Step 2:
Follow the instructions in the app until you reach the login page

Step 3:
Log in with your ABUS Single Sign-On details (partner access)
If you do not have an account, create a (free) account by clicking on the "Register" button.

Step 4:
After logging in, you will see the control panel overview. Add a new control panel using the plus button.

Step 5:
If you are commissioning the system for a customer, select "I am an installer". This creates you as an installer.
If you are installing the system for yourself, select "I am a user". This creates you as the Admin role with Installer & Admin rights.

Step 6:
Scan the QR code on the back of the control panel.

Note	Make sure that the system is connected to the internet.

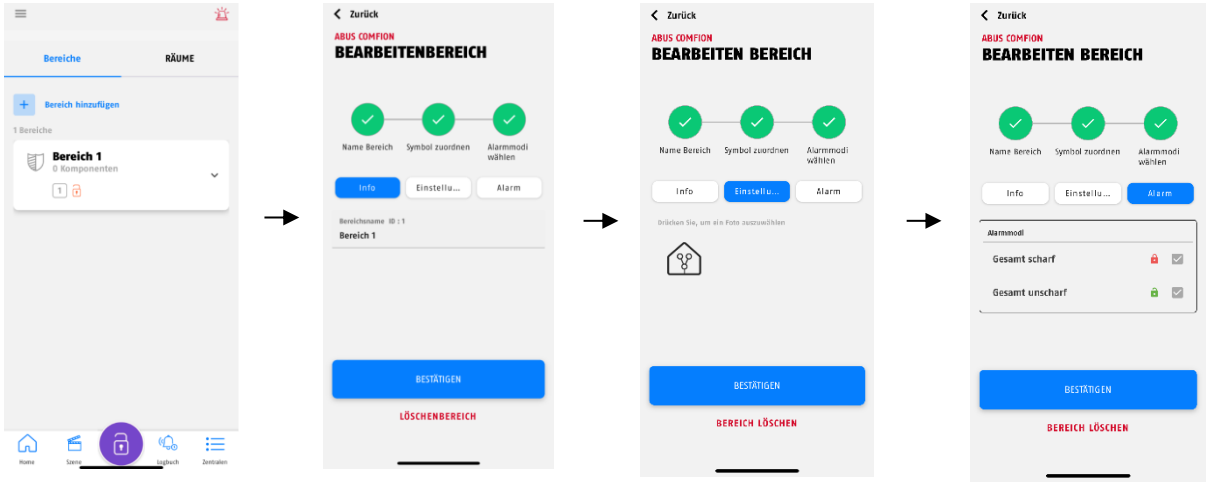
Step 7:
Assign a control panel name and confirm. The system will now start a firmware update before you can access the system. The firmware update may take a few minutes and involves restarting the control panel. The Power LED flashes orange during the update.

Step 8:
After restarting the control panel, the system is no longer greyed out in the control panel overview and can be called up by clicking on it.

3.2.3. Partitions

Partitions give you the option of dividing up the object to be monitored and thus being able to arm and disarm in a differentiated way. In conjunction with the alarm modes, you can switch partitions together or separately.

In the factory state, the system has one preconfigured partition. You can edit this partition by a long-press on it.



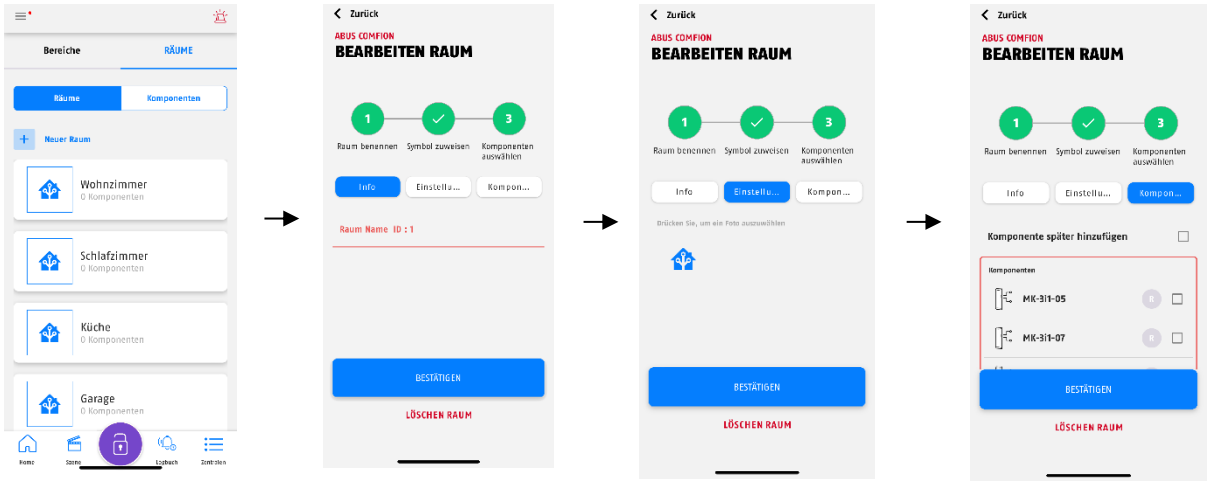
You can create additional partitions by clicking on the "Add new Partition" button.

With the Comfion wireless security system, it is advisable to divide the facade and interior into individual partitions. These can then be armed as required using the freely configurable alarm modes.

3.2.4. Rooms

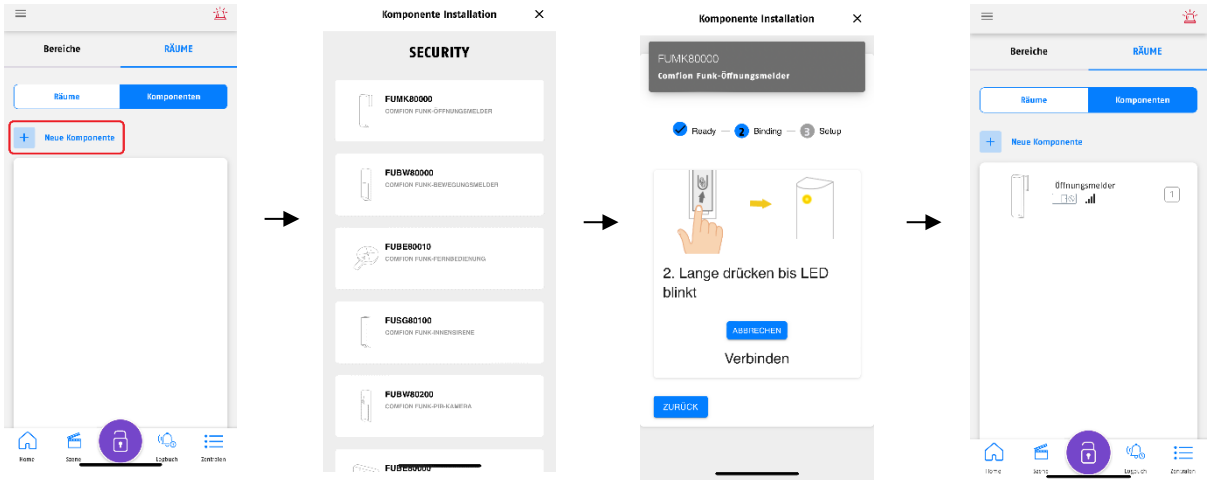
The Comfion wireless security system offers you the option of assigning your components to rooms. This serves to simplify the identification of components and has no functional properties. Rooms are not assigned to partitions, which means you can have components from different partitions in one room.

In the factory state, the system has a number of predefined rooms. You can freely edit these rooms or delete them completely. You can edit this partition by a long-press on it.



3.2.5.Components

The "Rooms" tab on the dashboard takes you to the component overview, where you will also find the "Add new Component" button. You can use this to add your Comfion products to the system.



With a long click, you can also edit a component that has already been connected and adjust the following device settings:

Temporary deactivation	OFF (default): Component functioning normally ON: Component is deactivated (no function)
Name	Component naming
Zone number	Assignment of the zone number (done automatically by the system)
Zone type	• Input *-> triggers an input delay, after which an intruder alarm is triggered* • Output -> *can be open during the output delay, functions like an immediate zone after arming* • Input/output -> *uses an input & output delay* • Immediate (intrusion) *-> triggers an intruder alarm when the system is armed* • Immediate (monitored) -> *works like the immediate zone when the system is armed; when the system is disarmed, a notification is sent when it is triggered* • 24-hour intruder alarm *-> intruder alarm independent of system status* • 24-hour water alarm *-> water alarm independent of system status* • 24 hour fire *-> fire alarm independent of system status* • Lock monitoring *-> Open zone prevents from setting but does not trigger an alarm when opened during armed system*
Zone behaviour	• Bypass *-> If the zone is triggered when armed, you have the option of bypassing it* • Transfer confirmation: If this item is activated, the signalling of zone alarms is delayed by the programmed time.

Note	If a detector is programmed for the zone type output or input/output, the system only checks the detector status after the delay time has elapsed when the system is armed. - If the detector is not ready after the time has elapsed and "Bypass" is activated, the detector is automatically bypassed after the delay time and the system is armed. - If the detector is not ready after the time has elapsed and "Bypass" is deactivated, the system is not armed.

3.2.6. Alarm modes

The Comfion wireless security system works with so-called "alarm modes", which form the core of the system. These are links between partitions and users for arming and disarming.

In an alarm mode, you define which user arms or disarms which partition with this alarm. This makes it possible to map all possible scenarios for arming and disarming.

In practice, a user is actually executing an alarm mode when arming or disarming.

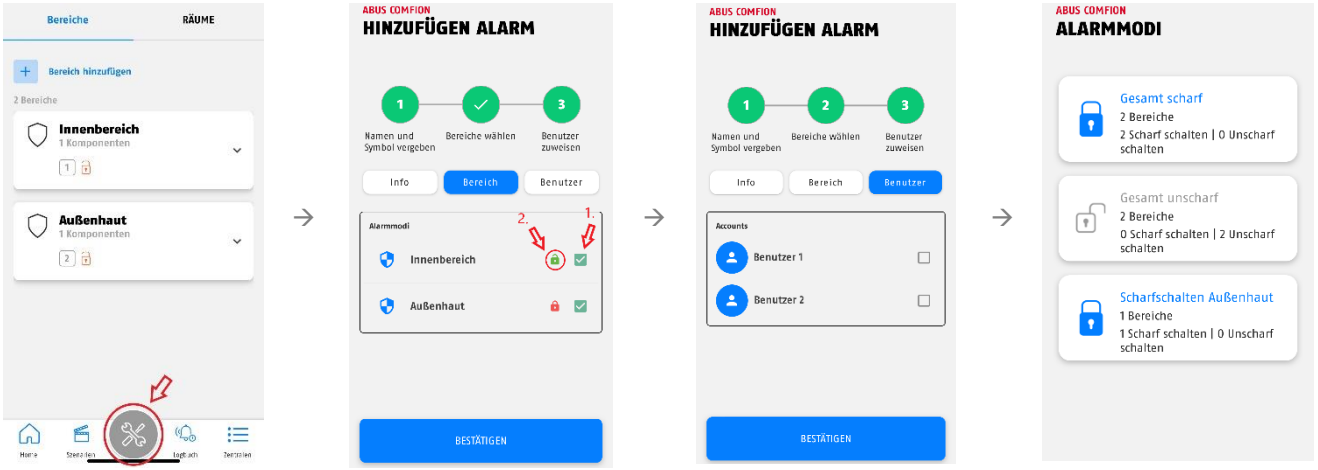
Note	The Comfion wireless security system has two preconfigured alarm modes in the factory settings: "Fully Arm" and "Fully disarm", which contain all the zones created.

Execution of an alarm mode

- The button at the bottom centre of the screen shows the current status of the system (armed, disarmed, partially armed or maintenance mode)
- By pressing the button, the available alarm modes are displayed and you can execute the corresponding switching command.

Creating or editing alarm modes

1. You can open the alarm mode management area by clicking on the bottom centre button as described in the previous step and then on the settings icon in the top right-hand corner of the screen.
2. Then click on "Add alarm mode" or edit an existing alarm mode by pressing and holding on it.
3. After you have assigned the name for the alarm mode, select the partitions AND the type of switching (armed or disarmed). To change the type of switching, click on the icon.
4. In the next step, select the users who should be authorised to switch this alarm mode.
5. After completion, the alarm mode appears in your overview and can be used.



3.3. Cameras (NVR)

Using the ONFIV integration protocol, various cameras from the ABUS Professional Line can be integrated into the Comfion wireless security system. You can integrate up to 4 cameras into the Comfion system and have them record (SD or SSD) if an event occurs, when the system is armed or continuously (24/7).

Note	A hard drive (SSD) is required in the control panel for continuous recording.

3.3.1. Integration of cameras

In the factory setting, the Comfion system automatically searches for ONFIV cameras in the network and adds them to the system. You can deactivate the automatic camera search in the camera overview in the camera settings.

Proceed as follows when integrating the cameras:

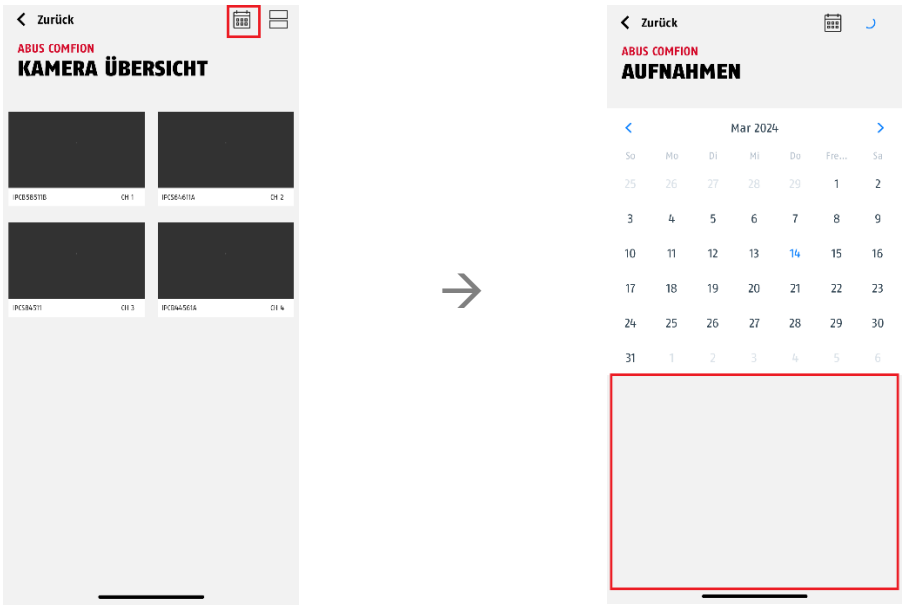
1. Integrate the camera into the same network as the Comfion.
2. Open the ABUS IP Installer and activate the camera.
3. Open the camera interface, log in as the installer and open the configuration.
4. In the advanced network settings under integration protocol, set ONVIF, save this setting and create an ONFIV user -> assign the same user name and password as an existing admin or installer for the camera.
5. Make the video settings in the camera described in the info-box below
6. Store the ONFIV user data in the Comfion system
7. Test the camera functions (live view, etc.)

Note	The following video stream settings are recommended depending on the number of integrated cameras (channels) in order to ensure an interference-free stream even when 4 channels are called up simultaneously and recorded continuously. Primary stream: • 1 channel: 1080p resolution; bit rate: 4096kbps • 2 channels: 1080p resolution; bit rate: 2048kbps • 3 channels: Resolution 1080p; bit rate: 1024kbps • 4 channels: Resolution 1080p; bit rate: 1024kbps Secondary stream: • 1-4 channels: Resolution: 360p; bit rate 512kbps

Note	• The max. resolution of 4MP per channel must not be exceeded • The max. bit rate must not exceed 4 x 2048kbps = 8192kbps at any time (all channels added up)

3.3.2. NVR operation

The surveillance view takes you to the parallel view of all channels. You can view the live image of all integrated cameras here. You can use the calendar function to view the existing recordings in the system sorted by date. The Comfion cuts the recordings into 15-minute clips.



By clicking on the respective camera stream, you can display the image in large format and access the specific functions of the camera (e.g. PTZ, 2WayAudio, etc.).

4. Users and permission types

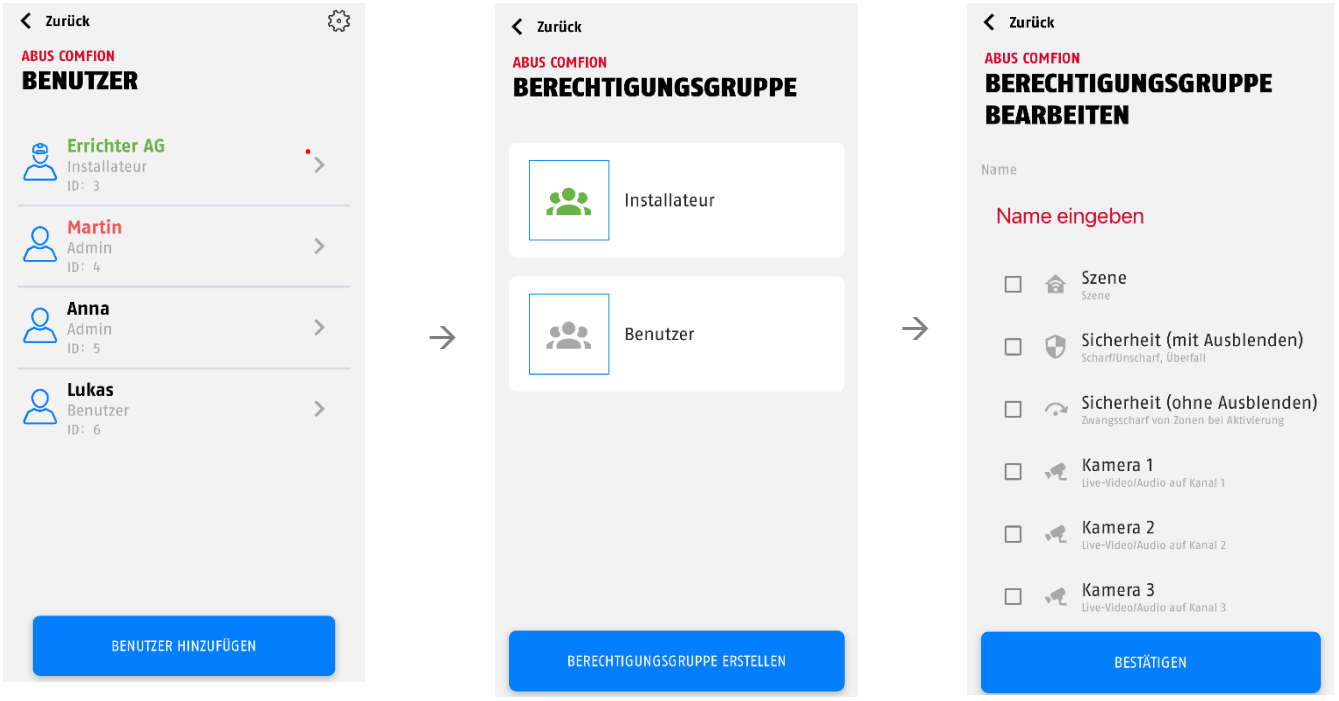
4.1. Explanation of the different roles

Installer	The installer has all user rights during initial commissioning. After handover of the system, the installer retains all configuration rights. The owner of the system can revoke the installer's rights to the live camera image and completely block access to the system.
Admin	The system admin has all user rights for the system. The admin can also create and edit automations and scenes. The installer also has the option of giving the admin configuration rights so that they have the rights of an installer.
Own role (user-defined)	You have the option of creating your own non-admin user groups and defining their permissions (see below)
Owner (additional role)	The owner role is automatically assigned to the first existing admin in the system. The owner role cannot be assigned manually. In addition to the admin permissions, the owner of the system has the permissions to add, invite and delete users. The owner of the system is highlighted in red in the user list.

The following setting options are available:

- Enable access: Blocks/gives access to the system and push notifications)
- Main installer: Determines which installer account the system is connected to for remote maintenance (installer portal)

Creating user groups:



4.2. Start-up

The "Installer" and "Admin" permission types are currently available in the factory settings of the control panel. If the system is commissioned by an installer, the installer initially has the permissions for all functions in the control panel.

4.2.1. Handover to the owner

Once you as the installer have completed the setup of the control panel, the system must be handed over to the end user. The first admin invited becomes the owner of the system. You can recognise this by the fact that this user is marked in red.
After inviting the owner, the installer loses the rights to edit and add users. Additional users must be added by the owner.

4.3. Inviting/adding users

New users can only be invited by the owner after handover. The following options are available when adding a new user:

- Invite a new user
  - Invite of a user based on the e-mail address.
- Selection from my members
  - Invite a member. Members can be added to the personal member list in the control panel overview. (See **6.3.2 Members**)
- Create a local user
  - Creation of a local user without an Abus Cloud account and without using the app. A remote control and a code for the keypad can be assigned to the user. You can also store a phone number and e-mail address for notifications.

The type of permission of the user to be added can also be selected. You can choose between Installer, Admin and the user groups you have created yourself.

4.4. Delete users

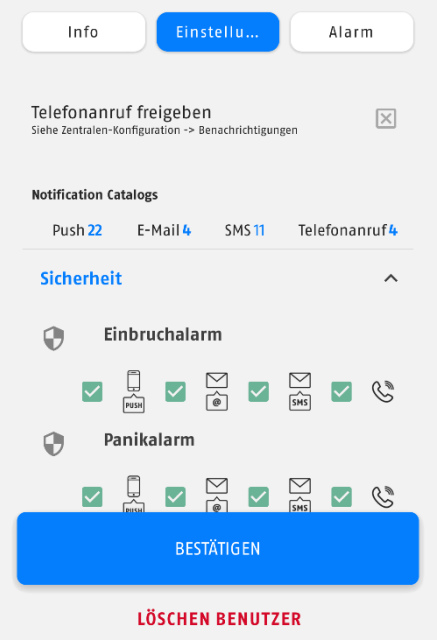
There are two ways to remove users from the control center:
1. the owner of the system (user marked in red) can remove any other user from the system by clicking on this user and the "Delete user" button.
2. Any user can delete themselves from the system by clicking and holding on the relevant control panel in the control panel overview and then confirming the request to delete.

Note	The owner of the system can only remove himself from the system in the second way (delete control panel from control panel overview). Once the owner has been removed, the role reverts to the installer. The installer can mark this as the new owner by inviting a new admin.

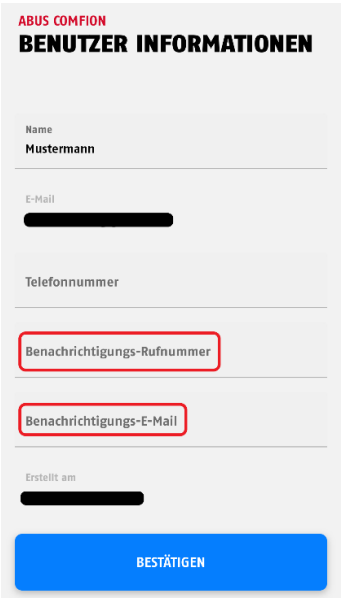
5. Communication

The Comfion security system has the following communication channels:
E-mail, push, SMS, phone call & control centre connection (SIA)

Under the "Users" menu item, you can select which notifications are to be sent for each event for each user created.



Your telephone number for SMS & telephone calls and your e-mail address for notifications are stored in your account. You can change these at any time. To do this, go to your control panel overview and click on the cogwheel in the top right-hand corner. You can now assign the notification phone number (**please include the country code e.g. +44**) and the notification e-mail address.



5.1. Modem

The Comfion security system has an integrated modem (2G/3G/4G). This can be used to send text messages and make calls in the event of an alarm. It also provides a redundancy path for the entire system communication. This means that if your internet connection fails, all communication with the cloud, including remote access and push notifications, is handled via mobile communication mode.

Note	Deactivate the PIN for your SIM card before inserting it into the modem. You can usually deactivate the PIN in the settings of any mobile phone.

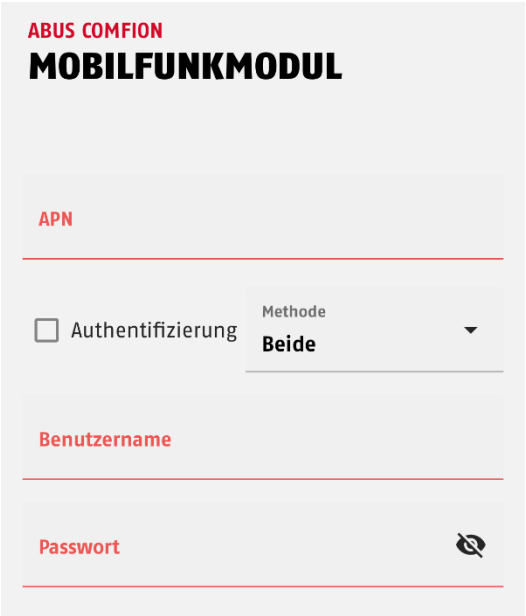
Note	Do not use SIM cards from abroad for permanent use in the Comfion.

A SIM card is required to operate the mobile communication mode. This SIM card can be chosen freely (recommendation ABUS: Telekom, Vodafone, o2) and must have the features you want to use on the control panel. If you want to use all the functions, you need a SIM card with text message capability, voice tariff and data volume.

Note	ABUS advises against using prepaid cards in the Comfion security system due to concerns about reliability. Furthermore, the use of multi-SIMs is not advisable as it can lead to connection problems.

RSSI-value	meaning
-109 to -95	bad
-93 to -85	low
-83 to -75	good
-73 to -53	excellent

No further settings need to be made in the modem itself for sending text messages or making calls. If you want to use the redundancy of the network services, it is necessary to store the APN data of the SIM card used. The menu item can be found under "Gateway configuration" – "Modem".



The APN data of your mobile phone provider is enclosed with your SIM card. Alternatively, you can check this online. The data is not SIM card-specific, but the same for every provider. If user name & password are specified in the APN data, tick the "Enable Authentication" box.

Example for telekom:

- APN: internet.telekom
- User name: t-mobile
- Password: tm

5.2. E-mail

Sending e-mails from Comfion works without configuration and is handled via the cloud.

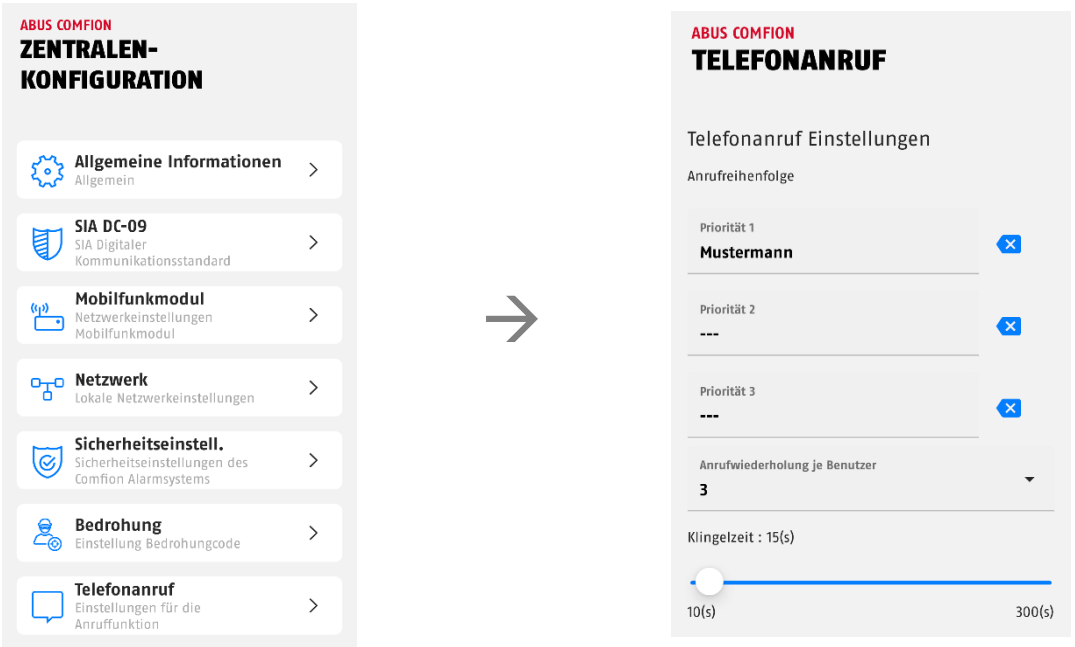
If the e-mail address to be notified differs from the account e-mail, you can store a notification address in your account (**see 5. Communication**). If you do not enter a notification e-mail, the e-mails will be sent to your account address.

5.3. Telephone call

The Comfion security system can call you in the event of an alarm. The system does not have a voice dialler, which means that no voice message is played for this call. The call is only for alerting purposes and is intended to help inform the called user of an alarm. The type of alarm can be seen from the push notification sent at the same time.

An inserted SIM card with call function and sufficient credit is required for the call function. Further information on the modem can be found in section **5.1 Modem**.

- To receive calls, the recipient's telephone number must be stored in the user account (see **5.** Communication).
- You must also define the call sequence under "Gateway configuration" – "Notification Voice". A maximum of 3 users can be called in succession.



Note	The number of call retries per user is set to 3 by default. This means that each user receives three calls. The call cannot be confirmed.

5.4. SMS

The Comfion system can send text messages (SMS) on the basis of the event list (see **5. Communication**). You can also use automated functions to send text messages with freely definable text for any event.

To be able to send text messages, a SIM card must be inserted in the modem and the notification number must be stored in the account (see **5. Communication**).

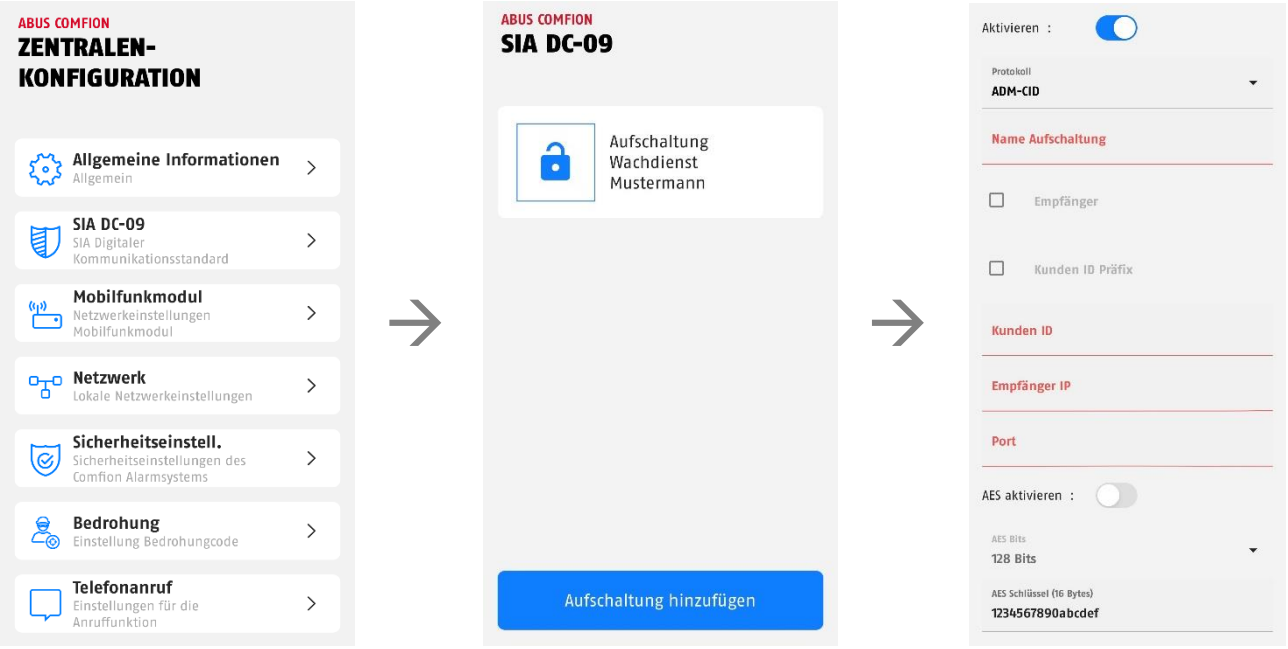
5.5. SIA DC-09 (control centre connection)

The Comfion wireless security system has a digital control centre dialler that can send the Contact-ID protocol using the SIA DC-09 standard. You can configure several SIA connections at the same time and thus communicate with different security services.

Enter the data received from your service provider in the relevant fields. The two greyed out fields "Receive No." and "Account Prefix" are generally not required and only need to be activated if explicitly requested by your service provider.

You can choose between the following options in the 'Static test message' field:

- **DC-09 Line monitorung** -> Supervision integrated in the DC-09-protocol (must be supported by the monitoring centre)
- **CID Testmessage 602** -> Transmission of the contact ID code 602 at the set interval



You can access the advanced settings via the symbol in the top right-hand corner of the screen.
Here you can activate the static test message and set the interval.

6. General information, maintenance and notes

6.1. Gateway configuration

Under the menu item Gateway configuration, you will find all the important information about your control panel and can also make important settings for the system

After you have called up the Gateway configuration menu item, you will see the following information:

- Control panel name (input field)
- Symbol (can be replaced by own photo)
- Network (display of the type of network connection)
- Mobile communication status (drop-down)
  - Module type (installed mobile communication chip)
  - SIM card (display whether inserted)
  - Phone call (display whether possible with inserted SIM)
  - Connection (display via connection status)
  - Signal strength (dBm)
- Power supply (display of mains adapter or battery)
- Firmware (click to display the version and release notes)
- Modem (display of the modem FW)
- Item number

You can open further settings menus via the cogwheel icon at the top right. The settings for SIA DC-09, telephone call and the modem can be found under 5. Communication.

6.1.1. General information

Information about the inserted storage medium (hard drive or SD card) is displayed under the "Memory" heading.

The time zone used and the NTP server are displayed under the heading "Date and time".

You can restart the system using the 'Restart' button.

6.1.2. Network

In this menu, you can view the network settings and adjust them if necessary.

You have three possible methods to choose from:
DHCP (default): Dynamic Host Configuration Protocol is a client/server protocol through which the Comfion is automatically provided with its IP address and other associated information by the router.

PPPoE: Point-to-Point Protocol over Ethernet is a network protocol that provides a direct connection in the internal network. This requires authentication by user name and password.

Static: If "Static" is selected, the Comfion network data is assigned manually. Discuss this with the network operator and do not assign an IP address from the DHCP pool.

Note	Incorrect IP settings mean that your system cannot connect to the network, making it inaccessible to the app. In this case, press the "connect" button on the back of the system for 6 seconds and then release it. The control panel will then restart and reset its network settings to the default DHCP settings.

6.1.3. Security Settings

Maintenance Mode	On/OFF (Default OFF)	Maintenance mode is used to install and maintain the system. The system cannot trigger any alarms while maintenance mode is active.
Zone lock	3x-20x (Default 5x)	If a zone is triggered more often than set, this zone will no longer trigger until the alarms are deleted from the alarm history
Keypad Retry Max	3x-20x (Default 5x)	Indicates after how many incorrect PIN entries on the control panel it is locked
Keypad Timeout	5-180 sec (Default 30 sec)	Time setting for how long the control panel is locked after X incorrect entries
Entry Delay	5-45 sec (Default 10 sec)	If the system is armed, the input delay is triggered by an input or input/output zone
Exit Delay	5-45 sec (Default 30 sec)	Time before the control centre changes to the armed state
Transmission delay	5-180 sec (Default 60 sec)	If this feature is activated in the zone, the transmission of a trigger is delayed by the set time.
Power Loss Report Delay	0-30 min (Default 0 min)	Adjustable delay for signalling a loss of voltage (12V DC)
Enable Intruder siren	On/OFF (Default AN)	Siren activation in the event of a burglar alarm
Intruder Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Enable Tamper Siren	On/OFF (Default AN)	Siren activation in the event of a tamper alarm
Tamper Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Enable Panic Siren	On/OFF (Default OFF)	Siren activation in the event of a hold-up alarm
Panic Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Enable Flood Siren	On/OFF (Default AN)	Siren activation in the event of a water alarm
Flood Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Enable Smoke Siren	On/OFF (Default AN)	Siren activation in the event of a fire alarm
Smoke Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Enable SOS Siren	On/OFF (Default OFF)	Siren activation in the event of a Panic alarm triggered via the app
SOS Siren Duration	5-180 sec (Default 60 sec)	Duration of acoustic signalling by sirens integrated into the system
Fault Override Network	On/OFF (Default OFF)	Detection and reporting of a network error
Fault Override Battery	On/OFF (Default OFF)	Detection and signalling of a battery fault
Fault Override AC Lost	On/OFF (Default OFF)	Detection and signalling of power loss (12V DC)
Fault Override Tamper SATA	On/OFF (Default OFF)	Detection and signalling of sabotage of the right-hand cover (hard drive)
Fault Override Tamper Case	On/OFF (Default OFF)	Detection and signalling of sabotage of the left cover (battery)

6.1.4.Alarm-Panel Backup

Note	For security reasons, the backup file of your alarm panel is stored fully encrypted in the Abus Cloud, exclusively on European servers.

Creating a Backup
Under the Backup menu in the Gateway Configuration, you can create a backup manually and activate the automatic backup. The automatic backup is performed weekly.

Importing a Backup
To import the backup into a new alarm panel, please proceed as follows:

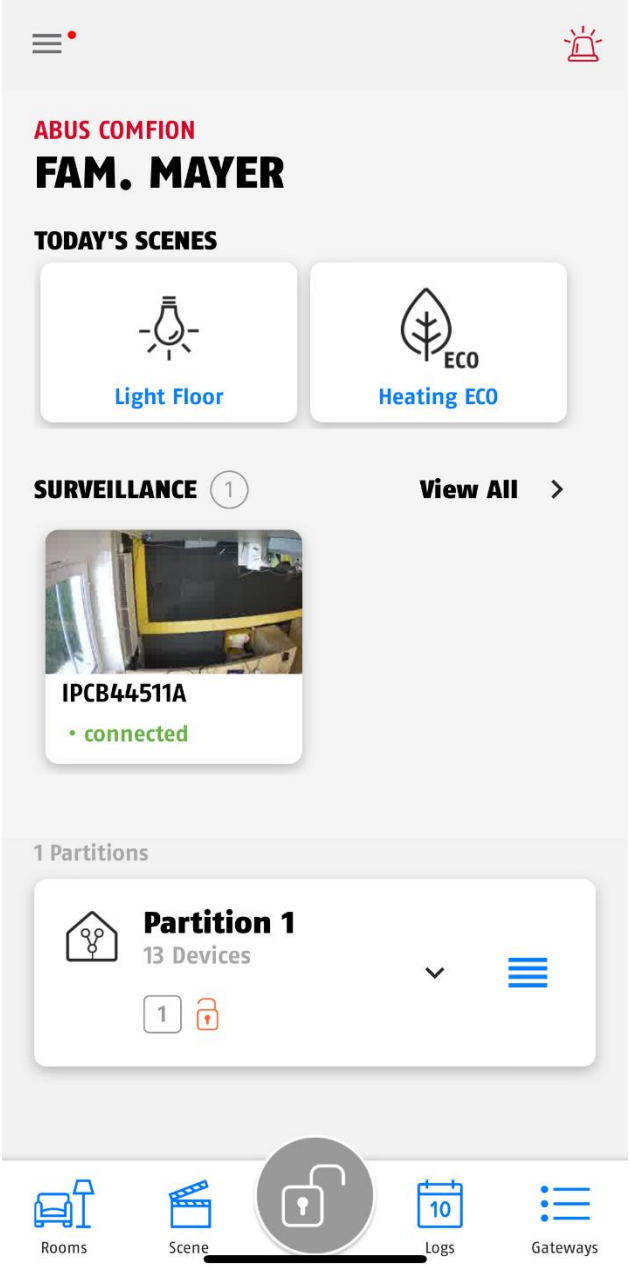
1. Disconnect the alarm panel from which the backup originates from the network, if you have not already done so, and switch it off.
2. In the gateway overview in the app, click on the + symbol to add a new Gateway.
3. Select 'Backup Import'
4. Scan the QR code on the back of your new alarm panel.
5. Select the alarm panel from which you want to load the backup.
   Note: After importing, the backup will be deleted from the cloud and the components will no longer work on the old alarm panel.
6. Enter the desired name of your new Gateway.
7. After confirmation, a verification code will be sent to the e-mail address of the owner of the system. Enter this code in the app and click on 'Start import'.
8. The import will now be carried out. You can now close your app and wait until you receive the push notification that the Gateway is online and the power supply is available.

To restore a configuration to the same hardware (Gateway), please proceed as follows:

1. Reset the affected Gateway to factory settings (press the reset button for 10 seconds -> see 6.5.1)
2. In the Gateway overview in the app, click on the + symbol to add a new Gateway
3. Select 'Backup Restore'
4. Scan the QR code on the back of your Gateway
5. Enter the desired name of your Gateway
6. The import will now be carried out. You can now close your app and wait until you receive the push notification that the alarm panel is online and the power supply is available.

6.2. Dashboard

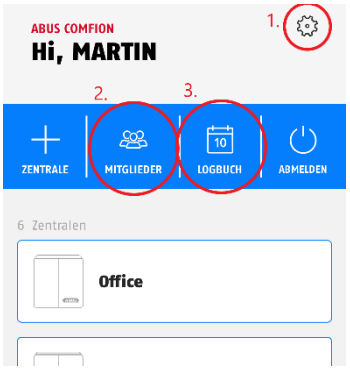
You can control the system via the dashboard and also carry out a large part of your work as installer.



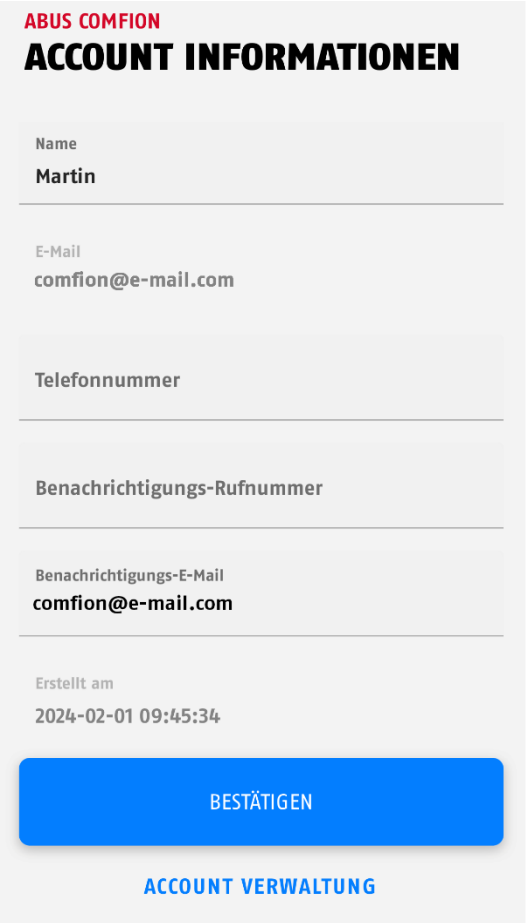
- ➔ Menu and panic button
- ➔ Gateway-Name
- ➔ Hotkeys – Can be edited under Scene-Menu
- ➔ Camera-Overview - Access to camera live streams and general camera settings
- ➔ Camera selection – Click on the respective camera to open the camera live stream directly
- ➔ Partition display. The partition can be edited with a long click. Click briefly to open the partition and display the assigned devices
- ➔ Manual sorting of the partitions by holding the button on the right
- ➔ Rooms = Display of the room overview & components
- ➔ Scene = Scenes and Autromations
- ➔ Logs = Display of the event memory
- ➔ Gateways = Gateway overview

6.3. Control panel overview

In the control panel overview of the system, you can view and access existing control panels, edit your account information (1), manage your members (2) and view the account log (3) in addition to adding new control panels.



6.3.1. User information



- ➔ Account name (displayed in control centre & logbook)
- ➔ Account e-mail
- ➔ Phone number
- ➔ Notification number for text message & phone calls
- ➔ Notification e-mail for e-mail transmission from the control panel
- ➔ Time of creation of the account
- ➔ Confirmation button to save the entries
- ➔ In-app deletion function of the ABUS account

6.3.2. Members

In the Comfion app, you have the option of keeping a list of members. This is purely optional and is not required to operate the Comfion systems. The member list allows you to easily select new users from your members when adding/inviting them to a control panel.

6.3.3. Account log

All messages from systems with authorised access are listed in the account log. If access to a system is blocked, log entries from this control panel are not saved in the account log.

6.4. Automations & scenes

The Comfion system offers you the option of configuring up to 100 scenarios. These scenes or automations can be set completely freely, giving you maximum flexibility.

You can add both scenes and automations under the "Scenes" tab.

Attention	Mutually contradictory or circularly calling automations must not be created. This can lead to serious functional problems with the control panel.

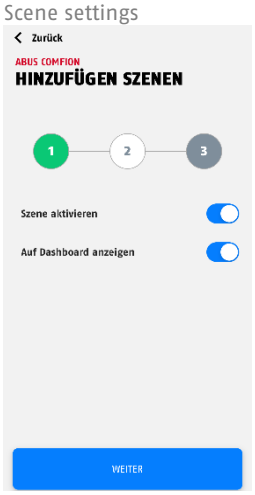
Attention	Make sure that you leave an interval of at least 5 seconds between two switching commands for the same device to ensure problem-free operation.

Scene = Action triggered by a user via the app (hotkey). Can be displayed in the dashboard.
Example: Socket ON/OFF via app

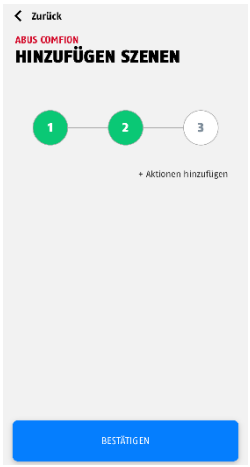
Example configuration of a scene:

Name / symbol assignment

Scene settings



Add action



Action selection

Automation = Always consists of if and then parts. Freely configurable.
Example: If system is armed, Then light off

In the If-part you can choose between an AND condition & an OR condition. With the AND condition, ALL conditions must be fulfilled for the action to be executed. At least ONE condition must be fulfilled for the action to be executed with the OR condition.

In the If section, you can choose between the following categories for the events:

- System -> Here you will find system events such as a power failure, but also the schedule
- Partition -> Partition events such as arming/disarming, intrusion, ready to arm and much more can be found here
- Zone -> All zone-related events can be found here (e.g. zone intrusion)
- Room -> All components and the associated events can be found here (e.g. opening detector contact opened or wall button pressed)

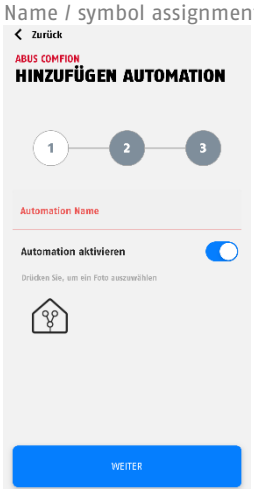
- Explanation "Advanced":
  Under "Advanced", you can set a time that defines how long the set conditions must apply before the action is executed. The action is only executed if the conditions apply for the set time period and no longer change.
  Example: If door is open for 30 seconds, Then send push notification

In the Then part, a distinction is made between

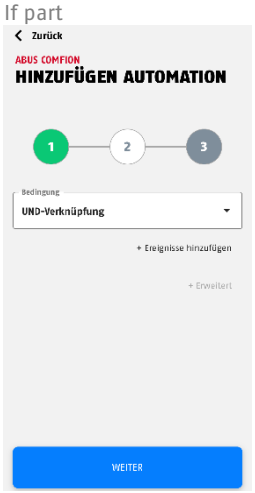
- "When conditions are met" -> Action is executed if the conditions specified in the If part apply
- "When conditions are not met" -> Action is executed if the conditions specified in the If part NO LONGER apply

Example configuration of an automation:

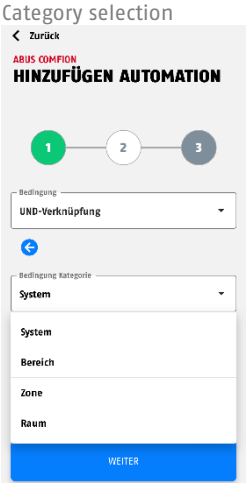
Name / symbol assignment



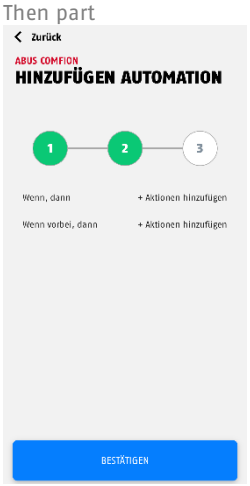
If part



Category selection



Then part



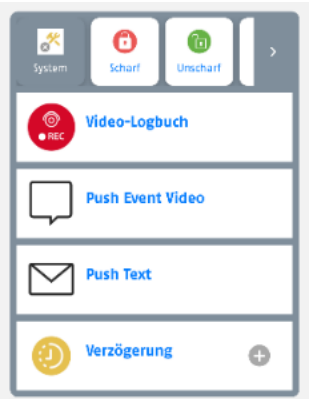
The following action selections are available if "System" is selected in the Then section of scenes or automations:

Video Log: Create a log entry (15 sec) with a section of the camera recording.

Push Event Video: Send a push message with definable text and section (15 sec) from the camera recording.

Push Text: Send a push message with definable text.

Delay: Adjustable delay in seconds - e.g. between two actions



Editing a scene/automation

To edit, press and hold the scene/automation icon for about 2 seconds and release it again

Deleting a scene/automation

You can delete a scene/automation by entering edit mode (see 'Editing a scene/automation') and then clicking on the 'Delete scene/automation' button at the bottom of the screen.

6.5. Resets

6.5.1. Factory Reset

To reset the system to factory settings, press and hold the reset button (see 2.3 Device description) for >10 seconds and release it again. The control panel LEDs will go out after a few seconds and the system will restart. After the restart, the alarm panel is reset to the factory settings and can be set up again.

6.5.2. User Reset

To reset the users of the system or delete all users from the system, press the left tamper contact (above the reset button) 5 times within 5 seconds. After a few seconds, the Internet LED briefly switches to red. You should receive a push notification on the connected devices that the relevant gateway has been removed.

When all LEDs are green again (Internet LED may flash green), you can add the system again using the + symbol in your app.

6.5.3. Network Reset

If you can no longer reach your system in the network due to incorrect IP settings, it is possible to reset your Comfion to DHCP. To do this, press and hold the network reset button on the back of the Gateway (labelled 'Connect') for 6 seconds. The system should be accessible again after a few minutes.

6.6. Function of the LEDs

Note	The LED displays listed below only apply after initial start-up of the system

Power LED: Shows the power supply status and can signal faults

Colour	Meaning
Green	Mains power supply
Red	Battery operation
Orange	Firmware update

Internet LED (globe): Shows the status of the cloud connection

Colour	Meaning
Green	Connected to the cloud (Owner is created)
Red	Connection to the cloud failed
Flashing green	Connected to the cloud (No owner created)

Network LED (arrows): Shows the communication channel currently in use

Colour	Meaning
Green	Connected to the internet via LAN
Red	3G/4G connection

Status LED (padlock): Shows system status

Colour	Meaning
Red	System armed
Orange	System partially armed
Green	System disarmed
Flashing green	Control panel is connecting to component

6.7. Operation

6.7.1. Arming / Disarming

- APP: Arming/disarming can be carried out in the app by executing the alarm modes. To do this, click on the central button at the bottom of the dashboard (lock symbol) and then select the action (e.g. fully arm).
- KEYPAD: You can arm and disarm the system using a wireless keypad. To do this, enter your user code and then click on the button (lock buttons). You can find more detailed information in the user guide or in the manual for the keypad
- KEYFOB: You can assign the alarm modes to the buttons on your wireless remote control and execute the respective action by pressing a button. The setting can be found under the keyfob.
- AUTOMATION: You can use automation to link the arming or disarming of the system to conditions. This can be used, for example, to switch according to a schedule or when a wire input is activated.

6.7.2. Restoring an Alarm

The Comfion system must be restored by the user after an alarm (intrusion, sabotage, etc.):

- The Comfion system automatically restores the alarm when it gets disarmed. As soon as all triggered detectors are back to normal status, the warning overview disappears from the dashboard.

6.8. Explanation of symbols

	Component triggered (e.g. window opened)
	Tampering (e.g. detector housing opened)
	Component activated (e.g. siren sound triggered)
	Component status OFF (e.g. wireless socket off)
	Component status ON (e.g. wireless socket on)
	Movement detected
	PIR camera: 1 Take photo (shutter button) 2 Photo is taken 3 Photo is transmitted
	Cable break (e.g. 3-in-1 detector)
	Power supply connected
	Wireless connection interrupted
	Zone closed
	Zone open
	Battery charge status
	4 bars = Excellent 3 bars = Very good 2 bars = Good 1 bar = OK 0 bars = Poor

6.9. ABUS Cloud

The Comfion wireless security system connects to the Abus Cloud during initial commissioning. The system is also stored in the installer's Abus Cloud installer account. If this is not desired, the "Main installer" checkbox can be removed under the respective user in the system, or can also be set for another installer.

6.10. Notes on the hard drive

- The screws for fastening the hard drive must only be tightened by hand
- The battery life of the control panel depends, among other things, on the hard drive installed and its power consumption, as well as the number of cameras and the selected recording type (continuous recording, etc.).
- The hard drive installed in the Comfion must be formatted in exFAT or NTFS format
- Only replace the hard drive when the control panel is de-energised

6.11. Service and maintenance by installers

Test that the system is working properly during routine maintenance:

- Check the Comfion system for obvious signs of damage to the housing or front cover.
- Check the action of the tamper switches (wall tear-off/housing cover left, housing cover right)
- Check the condition of the backup battery
- Clean the housing
  - To clean, please wipe the surface with a soft, dry cloth.
  - Do not use any water, solvents or cleaning agents.
- Check the signal strength and battery/rechargeable battery status of all components
- Replace the batteries as recommended by the manufacturer
- Test every component.
- Carefully clean the lenses on all PIR detectors and cameras using a soft, clean, dry cloth.
  - Do not use any water, solvents or cleaning agents.
- Carry out a walk test of all detectors.
- Test all sounders
- Test the communication.

Note	ABUS recommends changing the system battery after a maximum of 3 years. A sudden drop in performance cannot be ruled out with longer running times.

How to change the control panel battery:

- Set the alarm panel to maintenance mode (security settings)
- Open the left housing cover
- Disconnect the power supply and the old battery from the control panel
- Wait for 30 seconds
- Reconnect the new battery and the power supply
- Close the cover of the system and then exit maintenance mode again

6.12. Radio signal strength table

The following table describes the meaning of the signal values of the Comfion radio components displayed in dBm.

RSSI-value (dBm)	Meaning	Display at the device
<= -100	Poor	0 bars
<= -96	OK	1 bars
<= -91	Good	2 bars
<= -86	Very good	3 bars
> -86	excellent	4 bars

7. Release history

7.1. Overview

Publishing date	Firmware-Version alarm panel	App Version IOS/Android
21.03.2024	1.0.4736	0.2.1360
26.03.2024	1.0.4751	unchanged
10.05.2024	1.0.4957	0.3.1401
02.07.2024	1.0.5150	0.5.1471
16.09.2024	1.0.5398	0.5.1575 / 0.5.1577
11.11.2024	1.0.5500	0.6.1626
15.11.2024	1.0.5510	Unchanged
18.02.2025	1.0.5727	0.6.1702
28.02.2025	1.0.5782	Unchanged
18.03.2025	1.0.5836	Unchanged

7.2. Release Notes

You can find the release notes for the latest firmware update in your Comfion app or at the following link:
https://l.ead.me/becYdV

8. Warranty

- ABUS products are designed and manufactured with the greatest care and tested according to the applicable regulations.
- The warranty only covers defects caused by material or manufacturing errors at the time of sale. If there are demonstrable material or manufacturing errors, the module will be repaired or replaced at the guarantor's discretion.
- In such cases, the warranty ends when the original warranty period of two years expires. All further claims are expressly rejected.
- ABUS is not liable for defects and damage caused by external influences (e.g. transport, use of force, incorrect operation), improper use, normal wear and tear or failure to observe these instructions and the maintenance instructions.
- In the event of a warranty claim, the original receipt with the date of purchase and a short written description of the problem must be supplied with the product.
- Should you discover a defect on your product that was already present at the time of purchase, please contact your dealer directly within the first two years.

9. Disposal instructions

Dispose of the device in accordance with EU Directive 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). If you have any questions, please contact the municipal authority responsible for disposal. Information on collection points for waste equipment can be obtained from your local authority, from local waste disposal companies or your retailer, for example.

10. Conformity

10.1. EU Declaration of Conformity

Hereby, ABUS Security Center GmbH & Co. KG declares that the radio equipment type FUAA80000 is in compliance with Directive 2014/53/EU and 2011/65/EU. The full text of the EU declaration of conformity is available at the following internet address: abus.com > Article search > FUAA80000 > Downloads

10.2. Conformity according to EN 50131

The FUAA80000 security system is certified to security grade 2 when properly installed in accordance with EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 and EN 50131-5-3:2017.

ABUS | Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Phone: +49 82 07 959 90-0

ABUS
Security Tech Germany

FUAA80000

MANUEL D'INSTALLATION

Système de sécurité sans fil Comfion

V2.0

1. Gésnéralités

1.1. Introduction

Nous vous remercions d'avoir choisi le **système de sécurité sans fil Comfion**, un produit ABUS Security Center (également « ABUS » en abrégé).

Le présent manuel contient des descriptions essentielles, des caractéristiques techniques, des aperçus et des informations complémentaires sur la configuration, la mise en service et l'utilisation du **système de sécurité sans fil Comfion.**

Les produits/systèmes décrits ici ne peuvent être installés et entretenus que par des personnes qualifiées pour la tâche en question. En général, le personnel qualifié pour l'installation et la maintenance du système consiste en un partenaire ABUS spécialisé et formé.

1.2. Utilisation conforme / Mentions légales

Il incombe à l'acheteur ou au client et à l'utilisateur final d'utiliser le produit d'une manière conforme à la législation. Conformément à la responsabilité du fabricant quant à ses produits, telle qu'elle est définie dans la loi sur la responsabilité du fait des produits, les présentes informations doivent être respectées et transmises aux exploitants et aux utilisateurs. Le non-respect de cette consigne libère ABUS Security Center de sa responsabilité légale.

Une utilisation non conforme ou inhabituelle, des travaux de réparation ou des modifications non expressément autorisés par ABUS ainsi qu'un entretien non conforme peuvent entraîner des dysfonctionnements et doivent être évités. Toute modification non expressément autorisée par ABUS entraîne la perte des droits liés à la responsabilité ou à la garantie, ainsi que tout droit à la garantie convenu séparément.

Les architectes, les planificateurs techniques de bâtiments et autres institutions de conseil sont tenus de se procurer, auprès d'ABUS, toutes les informations nécessaires sur les produits, afin de satisfaire aux obligations d'information et d'instruction découlant de la loi sur la responsabilité du fait des produits. Les commerçants spécialisés et les installateurs sont tenus de respecter les consignes figurant dans la documentation ABUS et, le cas échéant, de transmettre cette dernière à leurs clients.

Vous trouverez de plus amples informations sur www.abus.com, page Généralités, ou, pour les revendeurs et les installateurs, sur le portail des partenaires à l'adresse suivante : https://partner-asc.abus.com/

1.3. Service clientèle / Customer Support

Pour toute aide supplémentaire, notre assistance est à votre disposition : support@abus-sc.com

1.4. Mentions légales

1. Édition française 05/2024

La parution d'un guide d'installation plus récent rend la présente édition caduque.

ABUS Security Center décline toute responsabilité quant aux erreurs de nature technique ou d'impression et quant à leurs conséquences. Les informations figurant dans le présent guide d'installation ont été rédigées de bonne foi et en tenant compte des connaissances techniques actuelles. Elles sont régulièrement contrôlées et, si nécessaire, mises à jour ou corrigées.

Est reconnu l'ensemble des marques et des droits de propriété intellectuelle, et des modifications peuvent être apportées sans préavis dans le cadre du progrès technique.

1.5. Signification des symboles

Les symboles suivants figurent dans le présent guide d'installation :

Symbole	Terme	Signification
	Prudence	Indique un risque de blessure ou de danger pour la santé dû à la tension électrique
	Important	Indique un risque d'endommagement de l'appareil/l'accessoire ou un risque de blessure ou un risque pour la santé
	Remarque	Indique des informations importantes

2. Principe de fonctionnement et caractéristiques de performance

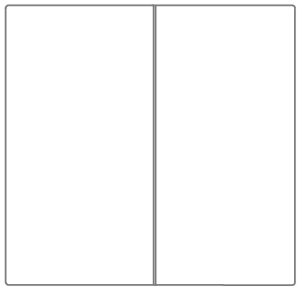
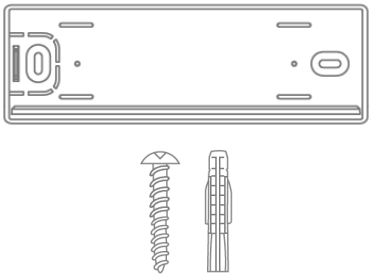
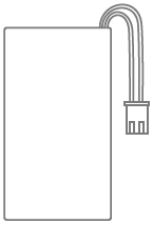
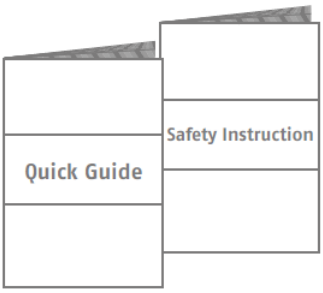
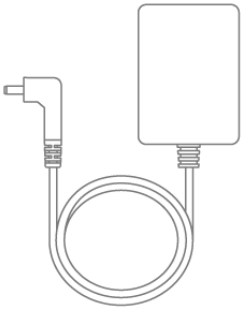
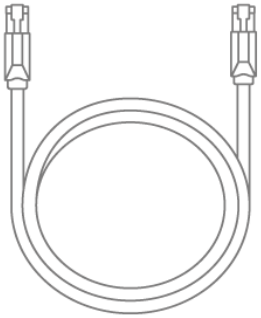
2.1. Caractéristiques du produit

Le **système de sécurité sans fil FUAA80000 Comfion** est un système de sécurité certifié EN degré 2 possédant des fonctions Smart Home. Le système peut être configuré et utilisé via l'application intuitive ou via le portail ABUS Cloud.

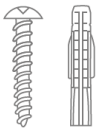
Caractéristiques principales :

- Montage facile : Grâce à l'absence de fil, les extensions ultérieures peuvent être mises en place à tout moment et à moindre frais
- NVR intégré : Jusqu'à 4 caméras pour l'enregistrement vidéo sur carte SD, ou 4 canaux NVR directement intégré à la centrale, intégration de caméras ABUS Professional Line
- Liaison radio 868 sûre, avec cryptage AES128 bit : Garantie d'une grande sécurité de transmission. De plus, l'aspect bidirectionnel du signal radio veille à ce que ce dernier soit bien arrivé à destination
- Jusqu'à 1 000 m de portée radio (champ libre)
- Surveillance anti-parasitage : Comfion émet une alarme lorsqu'un brouilleur est détecté
- Un seul système pour de nombreuses possibilités : 160 appareils, 50 utilisateurs, 40 partitions, 100 scénarios
- Sécurité pour votre client et pour l'assurance : Certification EN degré 2 de tous les composants de l'alarme
- Recours à un service de sécurité : Protocole de centrale de contrôle intégré (SIA DC-09)
- Communication et accès : Module de téléphonie mobile intégré (2G/3G/4G), pour une communication avec sécurité intégrée, une alarme et un accès à distance, même sans connexion Internet sur le site
- Toutes les informations sont toujours à portée de main : Notifications au choix : SMS, e-mail ou push

2.2. Contenu de la livraison

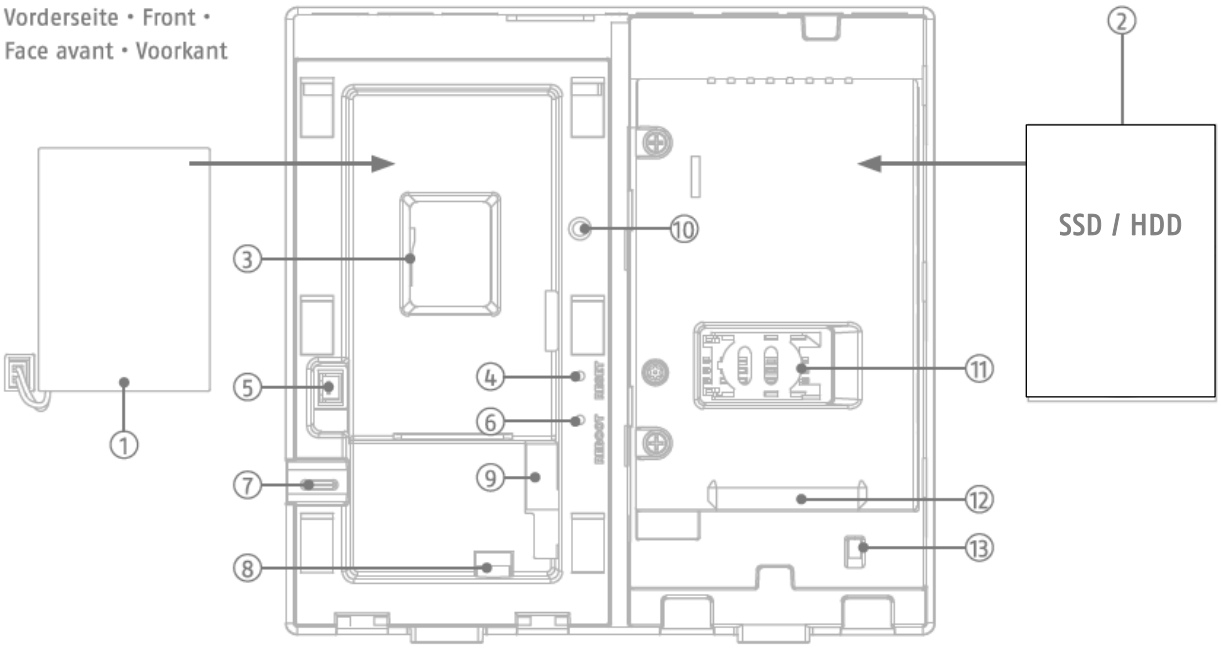
		
1 x centrale	1 x support mural 2 x vis	1 x batterie
		
Guide de démarrage rapide & consignes de sécurité	1 x adaptateur secteur	Câble LAN

Necessite:

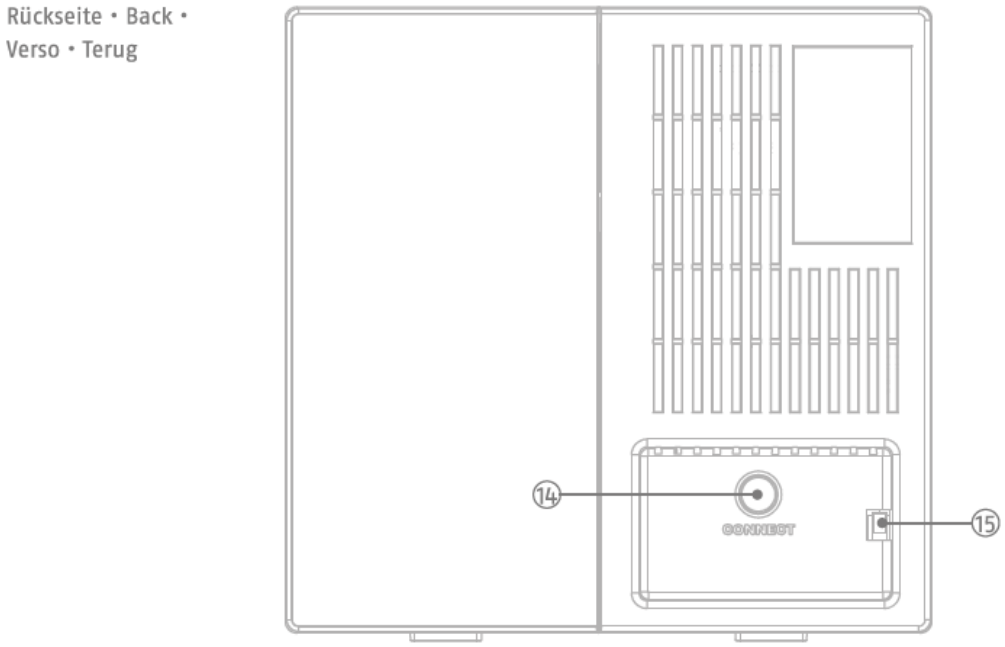

2 x vis/chevilles Ø 7.0 mm (M4)

2.3. Description de l'appareil

Structure du produit



1. Batterie de secours
2. Disque dur (non inclus)
3. Emplacement pour carte MicroSD
4. Bouton de réinitialisation
5. Connexion pour batterie de secours
6. Bouton de redémarrage
7. Passage de câbles
8. Connexion de l'alimentation externe
9. Prise RJ45
10. Interrupteur anti-sabotage (gauche)
11. Emplacement pour carte SIM (mini-SIM)
12. Connexion pour disque dur SATA
13. Interrupteur anti-sabotage (droite)
14. Bouton de réinitialisation du réseau
15. Interrupteur anti-sabotage (mural)



Oberseite • Top •
En haut • Top

16. Témoin LED d'alimentation
17. Témoin LED Internet
18. Réseau LED
19. Témoin LED d'état

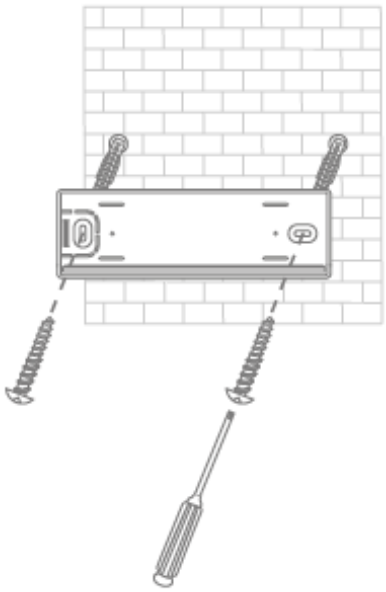
2.4. Caractéristiques techniques

Dimensions (l x H x P)	165 x 165 x 61 mm
Poids	596 g (avec batterie de secours et sans disque dur)
Température de service	-10 °C à +40 °C
Catégorie environnementale	II (EN 50131-1 + A3:2020)
Humidité de l'air	max. 85 % (relative)
Raccords	Prise 12 V DC, RJ45 (LAN), port SATA, emplacement pour carte SIM, emplacement pour carte Micro-SD
Témoins	LED d'état (alimentation, Internet, réseau, état du système)
Boutons	Bouton de redémarrage, bouton de réinitialisation
Fréquence radio / modulation	868.0 - 868,6 MHz / GFSK
Puissance, radio / portée	max. 25 mW (14 dBm) / 1000 m, champ libre
Nombre de composants radio	160
Nombre de partitions	40
Nombre d'utilisateurs	51
Nombre d'événements	> 10 000
Communication	Interface réseau : Ethernet 10/100 Mbps SSL/TLS Réseau mobile (sauvegarde) : 3G UMTS / 4G LTE SMS & appel : 2G GSM
Alimentation électrique	Primaire : Bloc d'alimentation 9 V DC / 2A, secondaire : Accu LiPo 7,4 V / 2 500 mAh
Type d'alimentation	Type A, alimentation conforme aux normes EN50131-1+A3:2020 et EN50131-6+A1:2021
Durée en mémoire tampon - fonctionnement sur batterie	> 12 heures selon EN50131-1+A3:2020 degré 2
Sécurité anti-sabotage (détection/protection)	oui (1x contact d'arrachement du mur ; 2 x contact de boîtier)
Durée de supervision	900 - 3 600 s (préréglage : 3 600 s)
Degré de sécurité	Degré 2 (EN 50131-1 + A3:2020)
Conformité	Degré de sécurité 2 en cas d'installation conforme au sens des normes EN 50131-1+A3:2020, EN 50131-3:2009 et EN 50131-5-3:2017
Directives européennes	RED : 2014/53/UE, RoHS : 2011/65/UE + 2015/863 Sécurité générale : 2001/95/CE

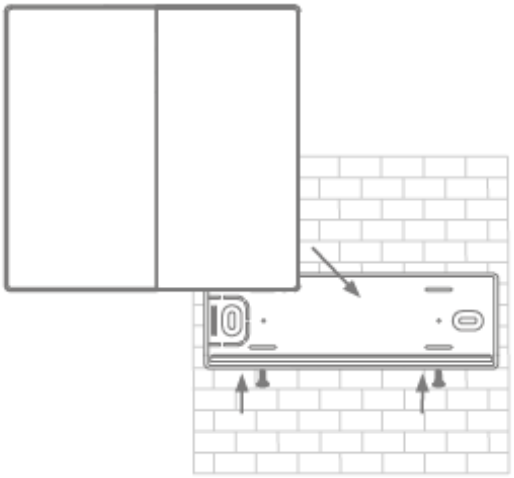
3. Montage et mise en service

3.1. Montage mural de la centrale

Remarque	- Montez la centrale au mur, à une hauteur d'environ 1,5 m - Maintenez une distance d'au moins 1 m de tous les côtés par rapport aux éléments suivants : appareils électriques, objets métalliques ou appareils émettant des ondes radio (par ex. routeurs, micro-ondes), car ces derniers peuvent affecter les performances radio du système.



Fixez le support au mur à l'aide des vis et des chevilles fournies.



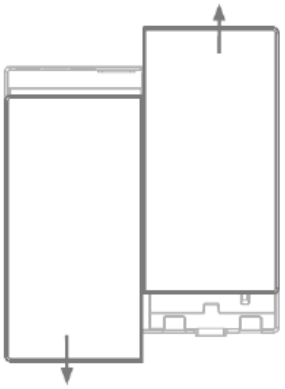
Placez la centrale sur le support mural et fixez-la avec les vis prémontées.

Remarque	Le retrait de la centrale de son support mural ou l'ouverture du couvercle de son boîtier déclenchent une alarme anti-sabotage. N'effectuez les travaux nécessaires sur le matériel que lorsque le mode maintenance est activé (*Configuration de la centrale -> Paramètres de sécurité*)

3.2. Mise en service du système

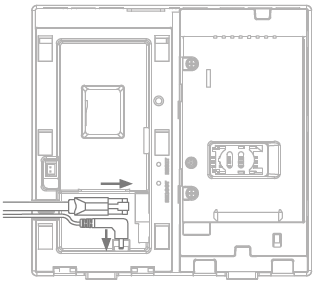
3.2.1. Préparation du matériel

- Faites glisser le couvercle gauche vers le bas et le couvercle droit vers le haut pour ouvrir le boîtier.



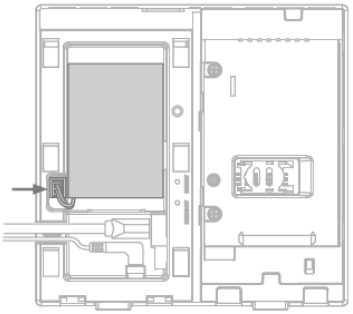
Remarque	Si vous souhaitez utiliser un disque dur, une carte SIM ou une carte SD, insérez-les avant de procéder à l'étape suivante (ajout de la tension secteur).

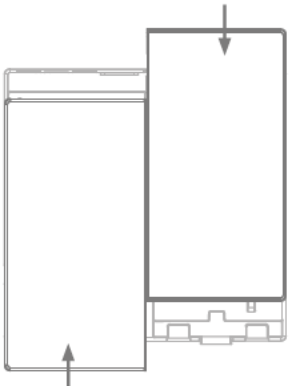
Remarque	Formatez votre carte SD ou votre disque dur au format exFAT ou NTFS avant de l'insérer. Il est interdit de travailler sur la carte SD ou le disque dur pendant le processus de démarrage de la centrale.



- Branchez le câble Ethernet et le câble réseau à la centrale pour établir la connexion électrique et la connexion réseau. Attendez que les 4 LED de la centrale s'allument (jusqu'à 40 secondes).

- Branchez la batterie de secours





- Fermez le boîtier à l'aide des deux couvercles avant

3.2.2. Installation via l'application

Remarque	La première mise en service de la centrale Comfion, et donc la connexion au portail des partenaires spécialisés et à l'installateur correspondant, doivent être effectuées via l'application.

Étape 1 :
Téléchargez l'application Comfion sur votre appareil mobile (IOS ou Android) depuis votre App-Store.

Étape 2 :
Suivez les instructions de l'application jusqu'à ce que vous arriviez à la page de connexion

Étape 3 :
Connectez-vous avec vos identifiants ABUS Single Sign-On (accès partenaire)
Si vous n'avez pas d'accès, créez un compte (gratuit) en cliquant sur le bouton « S'inscrire ».

Étape 4 :
Lorsque vous vous serez connecté, vous verrez l'aperçu de la centrale. Ajoutez une nouvelle centrale en cliquant sur le bouton « plus ».

Étape 5 :
Si vous mettez l'installation en service pour un client, sélectionnez « Je suis un installateur ». Vous aurez ainsi le rôle d'installateur. Si vous installez l'installation pour vous-même, sélectionnez « Je suis un utilisateur ». Vous aurez ainsi le rôle Admin et profiterez des droits d'installateur et d'administrateur.

Étape 6 :
Scannez le code QR au dos de la centrale.

Remarque	Veillez à ce que l'installation soit connectée à Internet.

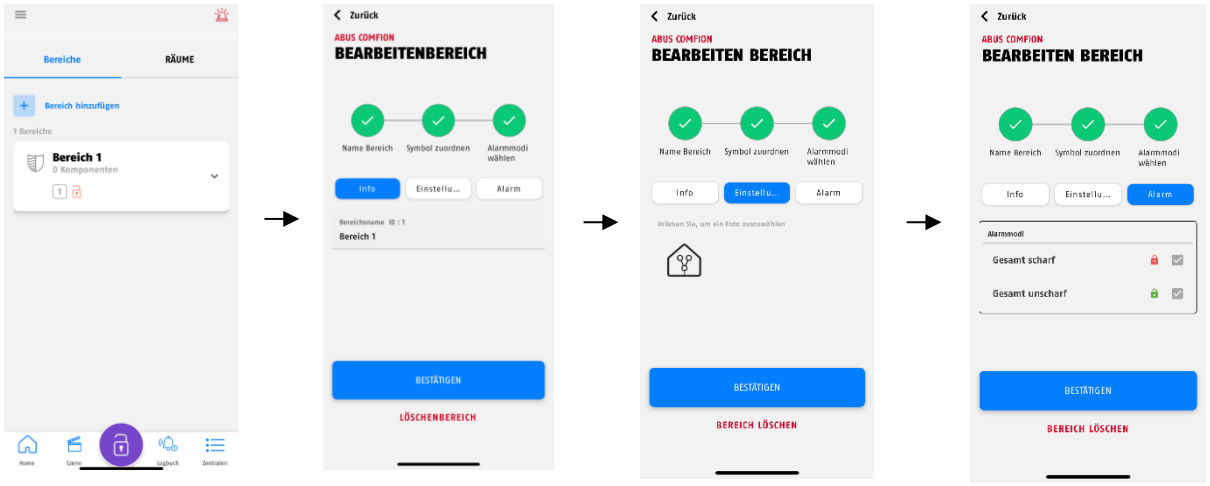
Étape 7 :
Attribuez un nom de centrale et confirmez-le. L'installation lancera alors une mise à jour du logiciel avant que vous ne puissiez accéder à l'installation. La mise à jour du logiciel peut prendre quelques minutes et entraîne un redémarrage de la centrale. La LED d'alimentation clignote en orange pendant la mise à jour.

Étape 8 :
Après le redémarrage de la centrale, l'installation n'est plus affichée en gris dans l'aperçu de la centrale.
Pour y accéder, il suffit alors de cliquer dessus.

3.2.3. Partitions

Les partitions vous donnent la possibilité de diviser le bâtiment à surveiller et ainsi d'armer ou de désarmer l'alarme. Dans ce contexte, les modes d'alarme vous permettent en outre de commuter des partitions en groupe ou individuellement.

Dans sa configuration d'usine, l'installation dispose d'une partition préconfigurée. Vous pouvez modifier cette partition en appuyant longuement dessus.



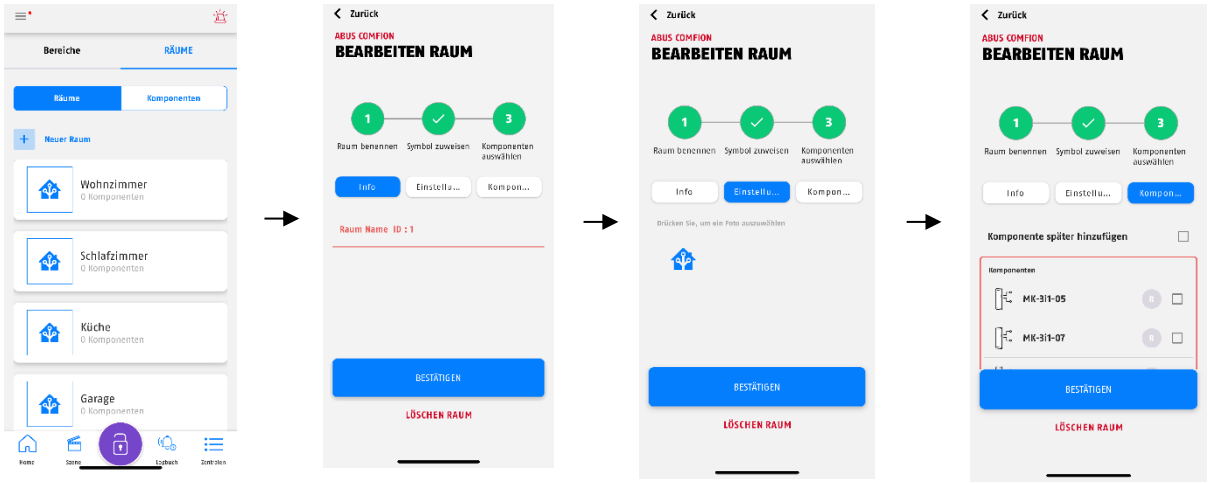
Pour créer d'autres partitions, il suffit de cliquer sur le bouton « Ajouter une partition ».

Avec le système de sécurité sans fil Comfion, il est recommandé de diviser l'intérieur et la façade en partitions distinctes. Celles-ci peuvent ensuite être armées à souhait via les modes d'alarme librement configurables.

3.2.4. Pièces

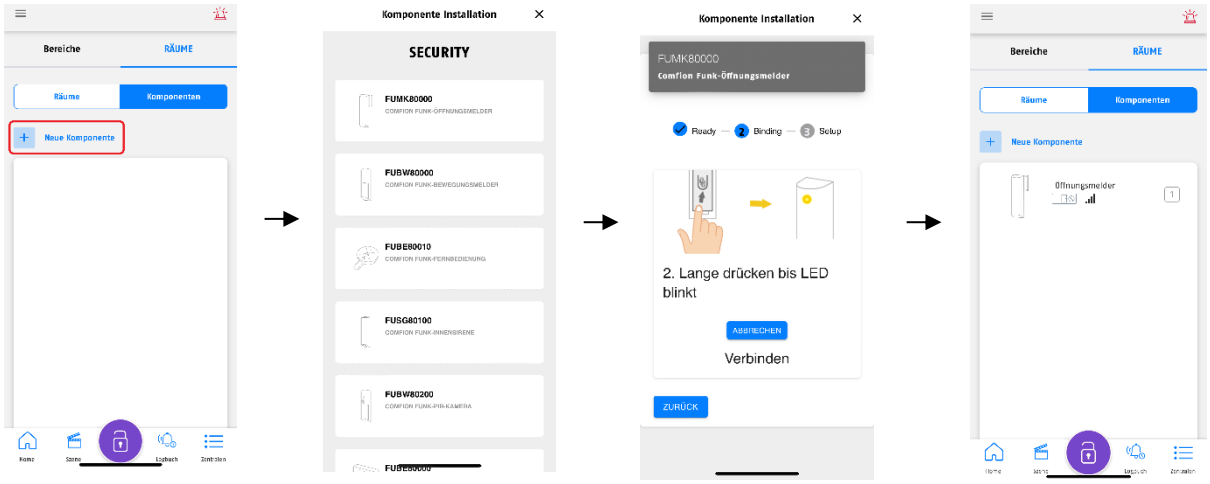
Le système de sécurité sans fil Comfion vous permet d'attribuer des composants aux pièces. Dépourvue de propriétés fonctionnelles, cette possibilité permet une identification plus facile des composants. Les pièces ne sont pas attribuées à des partitions, ce qui signifie que vous pouvez avoir des composants de différentes partitions dans une pièce.

Dans sa configuration d'usine, l'installation dispose de quelques pièces prédéfinies. Vous pouvez modifier librement ces pièces, ou encore les supprimer complètement. Vous pouvez modifier cette partition en appuyant longuement dessus.



3.2.5.Composants

L'onglet « Pièces » du tableau de bord vous permet d'accéder à l'aperçu des composants, où se trouve également le bouton « Nouveau composant ». Celui-ci vous permet d'ajouter vos produits Comfion au système.



Un long clic sur un composant déjà appris vous permet en outre de modifier et d'adapter les paramètres suivants du dispositif :

Désactivation temporaire	AUS (par défaut) : Composant en fonctionnement normal ON : Composant désactivé (aucun fonctionnement)
Nom	Attribution d'un nom au composant
Numéro de zone	Attribution d'un numéro de zone (automatiquement effectuée par le système)
Type de zones	• Entrée *-> déclenche une temporisation d'entrée, une alarme d'intrusion est déclenchée une fois le délai de temporisation écoulé* • Sortie -> *peut être ouverte pendant le délai de sortie, fonctionne comme une zone immédiate après l'armement* • Entrée/Sortie -> *utilise une temporisation d'entrée/un délai de sortie* • Immédiat (intrusion) *-> déclenche une alarme d'intrusion lorsque l'installation est armée* • Immédiat (Surveillé) -> *fonctionne comme la zone immédiate lorsque l'installation est armée ; si elle ne l'est pas, une notification est envoyée en cas de déclenchement* • Alarme d'intrusion 24 h/24 *-> Alarme d'intrusion indépendante de l'état de l'installation* • Alarme dégâts des eaux 24 h/24 *-> Alarme dégâts des eaux indépendante de l'état de l'installation* • Alarme incendie 24 h/24 *-> Alarme incendie indépendante de l'état de l'installation* • Surveillance des serrures *-> La zone ouverte empêche l'armement, mais ne déclenche pas d'alarme*
Comportement des zones	• Masquable *-> Si la zone est déclenchée avec armement, vous avez la possibilité de la masquer* • Confirmation de transmission : Lorsque ce point est activé, le message d'alarme de zone est retardé de la durée programmée.

Remarque	Si un détecteur est programmé sur le type de zone Sortie ou Entrée/sortie, l'installation armée ne vérifie l'état du détecteur qu'après l'expiration du délai de temporisation. - Si le détecteur n'est pas prêt à la fin du délai et que « Masquable » est activé, le détecteur est automatiquement masqué une fois le délai écoulé, et le système est armé. - Si le détecteur n'est pas prêt à la fin du délai et que « Masquable » est désactivé, le système ne s'arme pas.

3.2.6. Modes d'alarme

Le système de sécurité sans fil Comfion fonctionne avec des « modes d'alarme », qui constituent le cœur du système. Il s'agit de liens entre partitions et utilisateurs qui peuvent être armés et désarmés.

Vous définissez ainsi quel utilisateur armera ou désarmera quelle partition dans un mode d'alarme ou un autre. Vous pouvez ainsi configurer tous les scénarios d'armement et de désarmement possibles.

En fait, dans la pratique, lorsqu'un utilisateur arme ou désarme le système, il exécute un mode d'alarme.

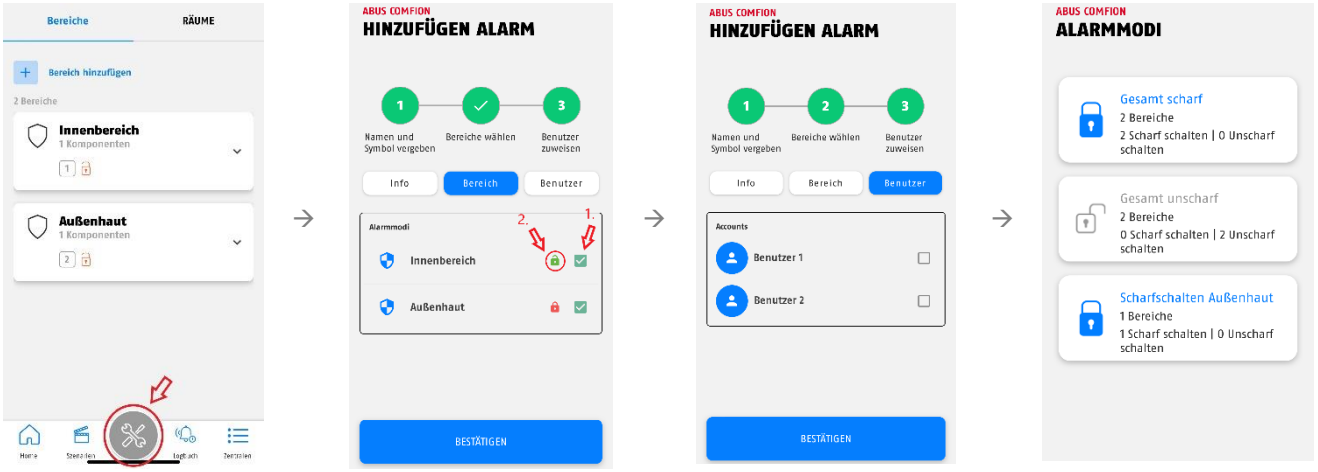
Remarque	Le système de sécurité sans fil Comfion possède deux modes d'alarme configurés par défaut : « Totalement armé » et « Totalement désarmé », qui contiennent toutes les partitions configurées.

Exécution d'un mode d'alarme

- Le bouton central situé en bas de l'écran indique l'état actuel de l'installation (armée, désarmée, armement partiel ou mode maintenance)
- Appuyez sur le bouton pour afficher les modes d'alarme existants et exécuter les activations souhaitées.

Créer ou modifier des modes d'alarme

1. Vous pouvez ouvrir le panneau de gestion des modes d'alarme en cliquant sur le bouton central inférieur (voir description à l'étape précédente), puis sur le symbole des réglages situé en haut à droite de l'écran.
2. Cliquez ensuite sur « Ajouter un mode d'alarme » ou modifiez un mode existant en appuyant longuement dessus.
3. Après avoir attribué un nom au mode d'alarme, choisissez les partitions ET le type d'activation (armé ou désarmé). Pour modifier le type d'activation, cliquez sur le symbole.
4. À l'étape suivante, sélectionnez les utilisateurs qui doivent avoir l'autorisation d'activer ce mode d'alarme.
5. Une fois terminé, le mode d'alarme apparaît dans l'aperçu et peut être utilisé.



3.3. Caméras (NVR)

Le protocole d'intégration ONFIV permet d'intégrer diverses caméras de la gamme ABUS Professional Line au système de sécurité sans fil Comfion. Vous pouvez intégrer jusqu'à 4 caméras à Comfion et les programmer de manière à ce qu'elles lancent un enregistrement (SD ou SSD) en cas d'événement, lorsque le système est armé, ou en continu (24h/24, 7j/7).

Remarque	L'enregistrement continu requiert la présence d'un disque dur (SSD) au sein de la centrale.

3.3.1. Intégration de caméras

Par défaut, le système Comfion recherche de manière autonome les caméras ONFIV du réseau et les ajoute au système. Vous pouvez désactiver la recherche automatique de la caméra sous l'aperçu caméra, dans les paramètres de la caméra.

Procédez comme suit pour intégrer les caméras :

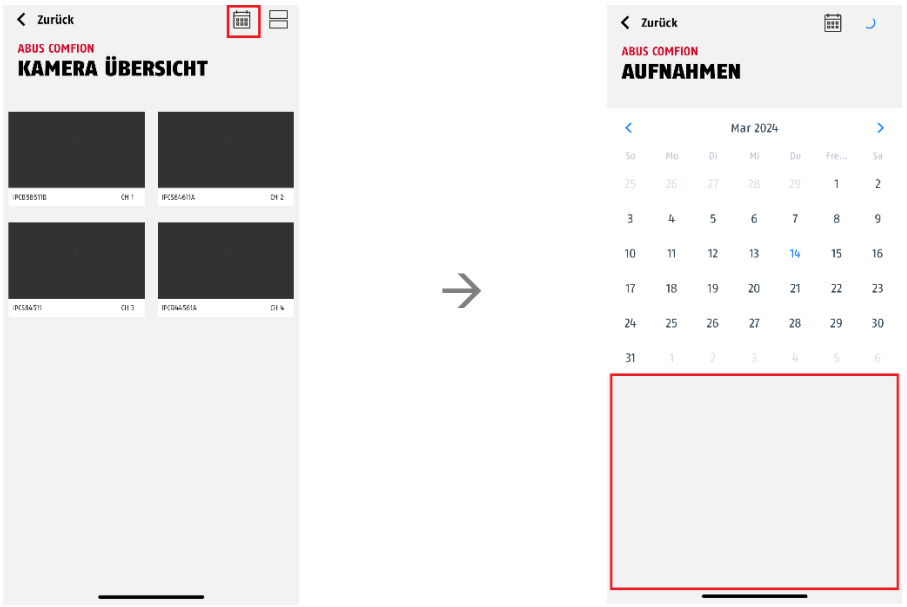
1. Connectez la caméra au même réseau que le système Comfion.
2. Ouvrez l'assistant d'installation IP ABUS et activez la caméra.
3. Ouvrez l'interface de la caméra, connectez-vous en tant qu'installateur et ouvrez la configuration.
4. Dans les paramètres réseau avancés, sous Protocole d'intégration, définissez ONVIF, enregistrez ce paramètre et créez un utilisateur ONFIV -> attribuez à la caméra le même nom d'utilisateur et le même mot de passe que deux d'un admin ou d'un installateur existant.
5. Effectuez les réglages vidéo décrits dans le champ de remarques ci-dessous dans la caméra
6. Enregistrez les données utilisateur ONFIV dans le système Comfion
7. Tester les fonctions de la caméra (image en direct, etc.)

Remarque	Les paramètres de flux vidéo suivants sont recommandés en fonction du nombre de caméras intégrées (canaux), afin de pouvoir garantir un flux sans perturbation même en cas d'appel simultané et d'enregistrement continu de 4 canaux. Flux primaire : • 1 canal : Résolution 1080p ; débit binaire : 4096kbps • 2 canaux : Résolution 1080p ; débit binaire : 2048kbps • 3 canaux : Résolution 1080p ; débit binaire : 1024kbps • 4 canaux : Résolution 1080p ; débit binaire : 1024kbps Flux secondaire : • 1-4 canaux : résolution : 360p ; débit binaire 512kbps

Remarque	• La résolution maximale de 4MP par canal ne doit pas être dépassée. • Le débit binaire maximal ne doit à aucun moment dépasser 4 x 2048kbps = 8192kbps (tous les canaux additionnés)

3.3.2. Utilisation du NVR

L'aperçu de la caméra vous permet d'accéder à la vue parallèle de tous les canaux. Vous pouvez y voir le flux en direct de toutes les caméras intégrées. La fonction calendrier vous permet de visionner les enregistrements stockés dans le système, triés par date. Le système Comfion découpe les enregistrements en clips de 15 minutes.



Cliquez sur un flux de caméra pour afficher l'image en grand format et accéder aux fonctions propres à la caméra (par ex. PTZ, 2WayAudio, etc.).

4. Utilisateurs et types d'autorisation

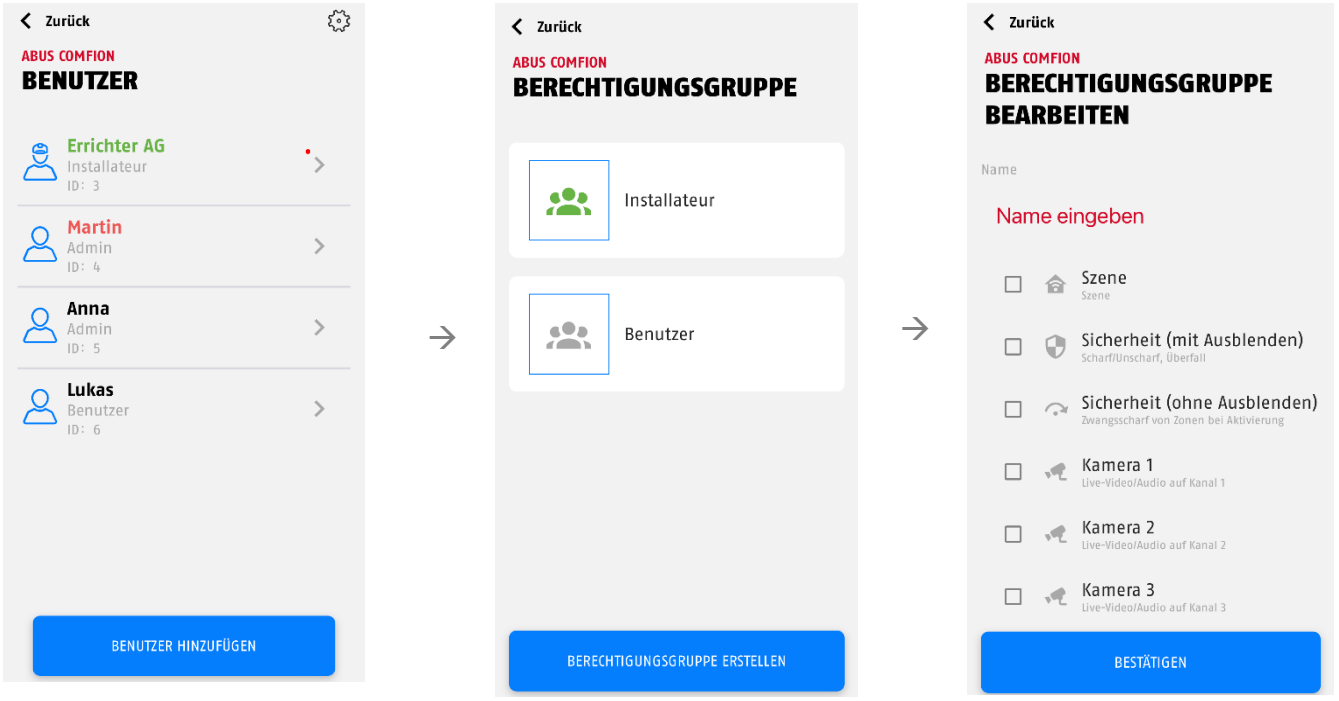
4.1. Explications sur les différents rôles

Installateur	L'installateur dispose de tous les droits d'utilisateur lors de la première mise en service. Après la remise de l'installation, l'installateur conserve tous les droits de configuration. Le propriétaire de l'installation peut retirer à l'installateur les droits relatifs à l'image en direct de la caméra et lui interdire complètement l'accès à l'installation.
Admin	L'admin de l'installation dispose de tous les droits d'utilisateur relatifs à cette dernière. Il peut également créer et modifier des automations et des scènes. L'installateur a en outre la possibilité d'attribuer des droits de configuration à l'admin, de sorte que celui-ci jouisse également des droits d'installateur.
Rôle propre (Personnalisé)	Vous avez la possibilité de créer vos propres groupes d'utilisateurs non-Admin et de définir leurs autorisations (voir ci-dessous)
Propriétaire (Rôle supplémentaire)	Le rôle propriétaire est automatiquement attribué au premier admin de l'installation. Le rôle propriétaire ne peut pas être attribué manuellement. Outre les droits d'Admin, le propriétaire de l'installation a le droit d'ajouter, d'inviter et de supprimer des utilisateurs. Le propriétaire de l'installation est indiqué en rouge dans la liste des utilisateurs.

Les options de paramétrage suivantes sont disponibles :

- Autoriser l'accès : bloque/autorise l'accès au système ainsi que les notifications push).
- Installateur principal : Définit le compte d'installateur avec lequel l'installation est reliée pour la télémaintenance (portail d'installateur spécialisé).

Création de groupes d'utilisateurs :



4.2. Mise en service

Dans sa configuration d'usine, la centrale compte les types d'autorisation « Installateur » et « Admin ». Si l'installation est mise en service par un installateur, celui-ci est autorisé, au début, à utiliser toutes les fonctions de la centrale.

4.2.1. Remise au propriétaire

Une fois que vous, l'installateur, avez terminé la configuration de la centrale, il convient de remettre l'installation à l'utilisateur final. Le premier admin invité devient le propriétaire de l'installation. Vous le reconnaîtrez au fait que cet utilisateur est indiqué en rouge.
Après avoir invité le propriétaire, l'installateur perd les droits de modification et d'ajout d'utilisateurs.
Les utilisateurs supplémentaires doivent être ajoutés par le propriétaire.

4.3. Inviter/ajouter des utilisateurs

Les nouveaux utilisateurs ne peuvent être invités que par le propriétaire après la remise. Lorsque vous ajoutez un nouvel utilisateur, vous avez le choix entre les possibilités suivantes :

- Inviter un nouvel utilisateur
  - Inviter un utilisateur via son adresse e-mail.
- Sélection de mes membres
  - Inviter un membre. Les membres peuvent être ajoutés à la liste personnelle des membres dans l'aperçu de la centrale. (Voir **6.3.2 Membres**)
- Créer un utilisateur local
  - Création d'un utilisateur local sans compte Abus Cloud et sans utilisation de l'application. L'utilisateur local peut se voir attribuer une télécommande et un code pour le clavier de commande. Il est également possible de saisir un numéro de téléphone et un e-mail pour les notifications.

En outre, il est possible de choisir l'autorisation de l'utilisateur à ajouter. Il est alors possible de choisir entre Installateur, Admin et les groupes d'utilisateurs créés.

4.4. Supprimer un utilisateur

Il y a deux possibilités pour supprimer des utilisateurs de la centrale :

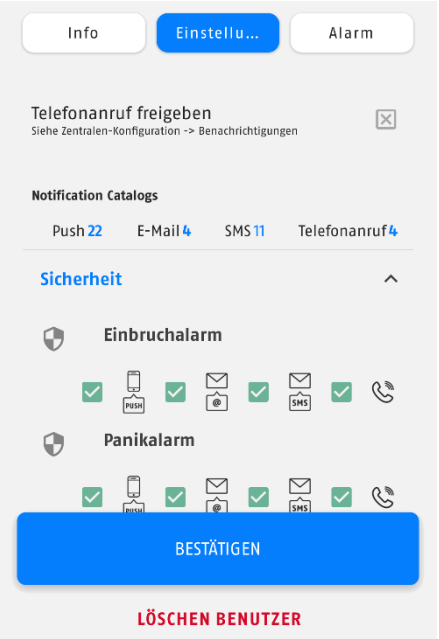
1. le propriétaire de la centrale (utilisateur marqué en rouge) peut supprimer tout autre utilisateur du système en cliquant sur celui-ci et sur le bouton « Supprimer l'utilisateur ».
2. Chaque utilisateur peut se supprimer lui-même de l'installation en cliquant longuement sur la centrale concernée dans l'aperçu des centrales et en confirmant ensuite la demande de suppression.

Remarque	Le propriétaire de l'installation ne peut se retirer lui-même du système que par la deuxième voie (supprimer la centrale de l'aperçu des centrales). Après la suppression du propriétaire, le rôle revient à l'installateur. Celui-ci peut, en invitant un nouvel administrateur, le désigner comme nouveau propriétaire.

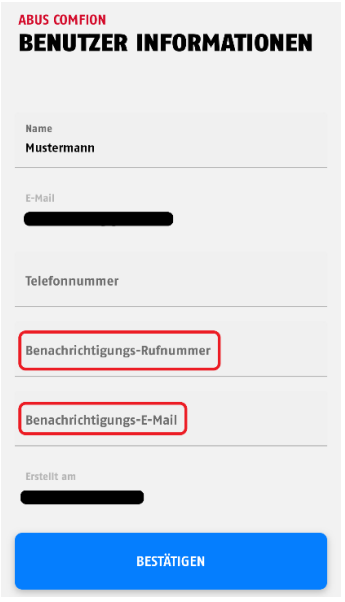
5. Communication

Le système de sécurité Comfion dispose des voies de communication suivantes : E-mail, notification push, SMS, appel & activation de la centrale de contrôle

Dans le menu, l'option « Utilisateurs » vous donne la possibilité de choisir, pour chaque utilisateur créé, les notifications qui doivent être envoyées en fonction d'un tel ou d'un tel événement.



Sont enregistrés dans votre compte votre numéro de téléphone (pour les SMS et les appels téléphoniques) et votre adresse e-mail (pour les notifications). Vous pouvez les modifier à tout moment. Pour ce faire, allez dans l'aperçu de la centrale et cliquez sur la roue dentée dans le coin supérieur droit. Vous pouvez maintenant attribuer le numéro de téléphone de notification ainsi que l'e-mail de notification.



5.1. Module de téléphonie mobile

Le système de sécurité Comfion dispose d'un module de téléphonie mobile intégré (2G/3G/4G). Celui-ci permet d'envoyer des SMS et de passer des appels en cas d'alarme. Il offre également une redondance pour toutes les communications du système. Cela signifie qu'en cas de panne de votre connexion Internet, toute communication avec le cloud, et donc l'accès à distance ainsi que les notifications push, sont gérés via le mode de téléphonie mobile.

Remarque	Désactivez le code PIN de votre carte SIM avant d'insérer cette dernière dans le module de téléphonie mobile. En règle générale, vous pouvez désactiver le code PIN dans les paramètres de n'importe quel téléphone.

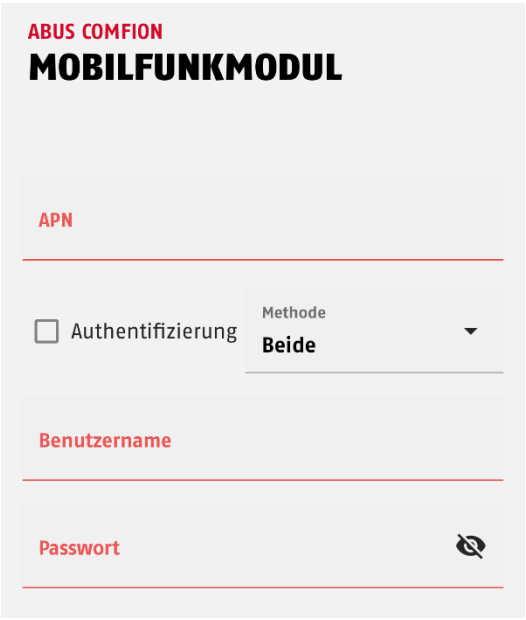
Remarque	N'utilisez pas de cartes SIM provenant de l'étranger avec le système Comfion à long terme.

Une carte SIM est nécessaire pour le fonctionnement du mode de téléphonie mobile. Cette carte SIM est libre de choix (recommandation ABUS : Telekom, Vodafone, o2) et doit présenter les fonctionnalités dont vous souhaitez disposer sur la centrale. Si vous souhaitez utiliser toutes les fonctions, vous avez besoin d'une carte SIM avec SMS, forfait appel et volume de données mobiles.

Remarque	Pour des raisons de fiabilité, ABUS déconseille d'utiliser des cartes prépayées avec le système de sécurité Comfion . En outre, il est déconseillé d'utiliser une deuxième carte SIM, qui peut entraîner des problèmes de connexion.

Valeur-RSSI	Signification
-109 à-95	Mauvaise
-93 à-85	Faible
-83 à-75	Bon
-73 à-53	Excellent

Aucun autre réglage ne doit être effectué au sein du module de téléphonie mobile pour l'envoi de SMS et les appels.
Si vous souhaitez profiter de la redondance des services du réseau, il est nécessaire d'enregistrer les données APN de la carte Sim utilisée. Vous trouverez l'option correspondante sous « Configuration de la centrale » - « Module de téléphonie mobile ».



Les données APN de votre opérateur de téléphonie mobile sont jointes à votre carte SIM. Vous pouvez également les consulter en ligne. Les données ne sont pas propres à la carte SIM, mais identiques pour chaque opérateur. Si le nom d'utilisateur et le mot de passe sont indiqués dans les données APN, cochez la case « Authentification ».

Exemple Telekom :

- APN : internet.telekom
- Nom d'utilisateur : t-mobile
- Mot de passe : tm

5.2. E-mail

Exécutée via le cloud, la fonction d'envoi d'e-mails du système Comfion ne requiert aucune configuration.

Si l'adresse e-mail à notifier doit être différente de l'adresse e-mail du compte, vous pouvez enregistrer une adresse de notification dans votre compte (**voir 5. Communication**). Si vous n'enregistrez pas d'adresse e-mail de notification, les e-mails seront envoyés à votre adresse de compte.

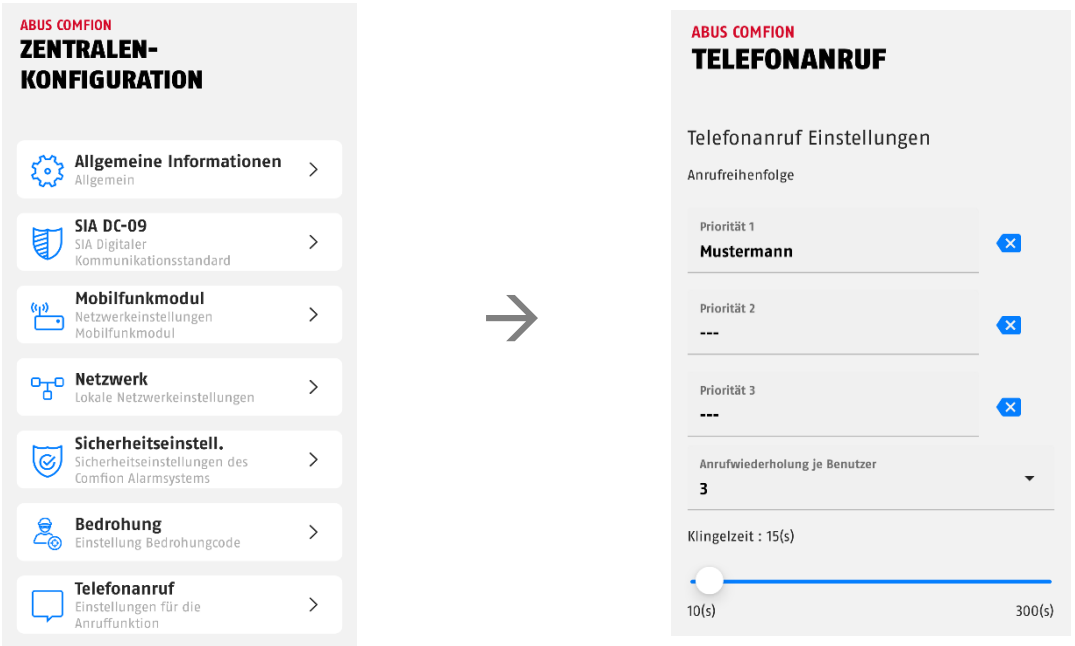
5.3. Appel téléphonique

Le système de sécurité Comfion est en mesure de vous appeler en cas d'alarme. L'installation ne dispose pas de numéroteur de messages vocaux, ce qui signifie qu'aucun message vocal ne sera joué lors de cet appel. L'appel sert uniquement à alerter et à informer l'utilisateur qui reçoit l'appel de l'alarme. La notification push envoyée simultanément indique le type d'alarme duquel il s'agit.

La fonction d'appel requiert l'insertion d'une carte SIM dotée de la fonction d'appel et de suffisamment de crédit. Pour plus d'informations sur le module de téléphonie mobile, voir **5.1 Module de téléphonie mobile.**

- Le numéro de téléphone du récepteur doit être enregistré dans son compte d'utilisateur pour que ledit récepteur puisse recevoir des appels (voir **5**. Communication).

- En outre, vous devez définir la séquence d'appels sous « Configuration de la centrale » - « Appel téléphonique ». Le système peut appeler jusqu'à 3 utilisateurs l'un à la suite de l'autre.



Remarque	La répétition des appels par utilisateur est réglée en usine sur 3. Cela signifie que chaque utilisateur reçoit trois appels. L'appel ne peut pas être confirmé.

5.4. SMS

Le système Comfion peut envoyer des messages SMS sur base de la liste des événements (voir **5. Communication**). En outre, les automations permettent d'envoyer des messages SMS avec un texte librement définissable en cas d'événements quelconques.

L'envoi de SMS requiert l'insertion d'une carte SIM dans le module et l'enregistrement,dans le compte, du numéro de téléphone de notification (voir **5. Communication)**.

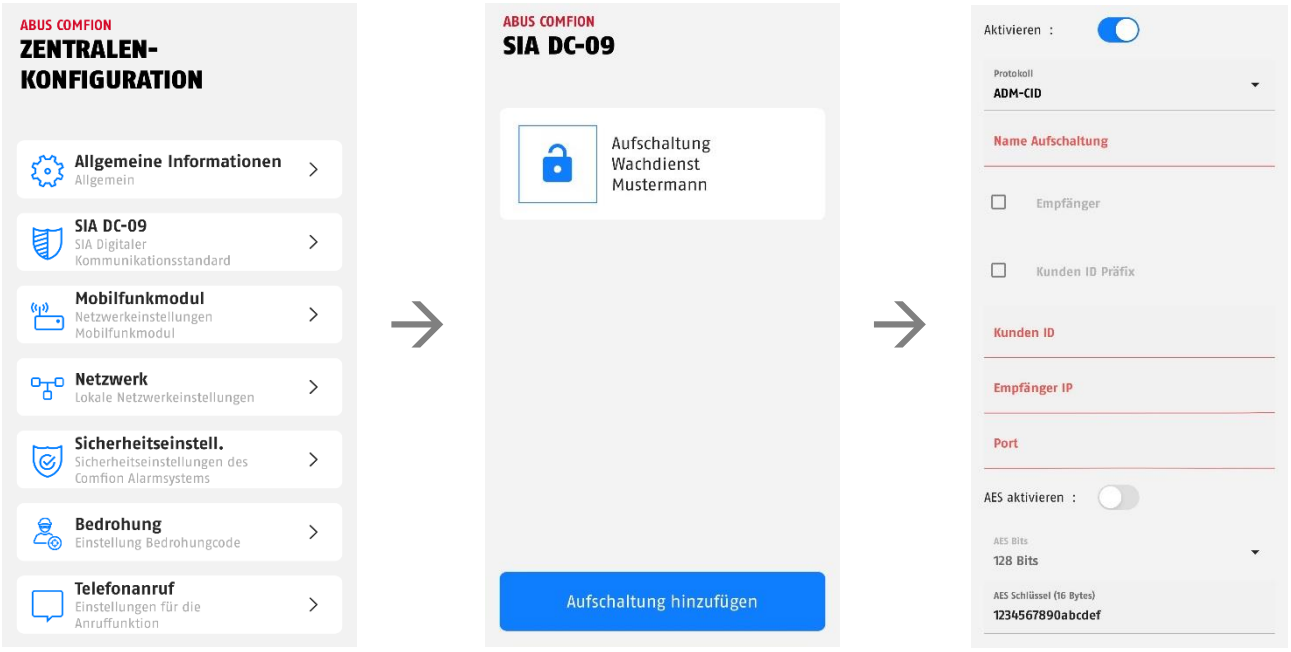
5.5. SIA DC-09 (activation de la centrale de contrôle)

Le système de sécurité sans fil Comfion dispose, pour la connexion à la centrale de contrôle, d'un numéroteur numérique capable d'envoyer le protocole Contact-ID via la norme SIA DC-09. Vous pouvez configurer plusieurs activations en même temps et assurer ainsi la communication avec différents services de sécurité.

Saisissez les données que votre prestataire de services vous a transmises dans les champs concernés. Les deux champs grisés « Récepteur » et « Préfixe de l'ID clienté » ne sont généralement pas nécessaires et ne doivent être activés que si votre prestataire de services le demande explicitement.

Dans le champ « Message de test statique », vous pouvez choisir entre les options suivantes :

- **DC-09 Supervision de la ligne** -> Supervision intégrée dans le protocole du poste de contrôle (doit être supporté par le poste de contrôle)
- **Message test CID 602** -> Transmission du code Contact-ID 602 à l'intervalle défini



Le symbole de la roue dentée en haut à droite de l'écran vous permet d'accéder aux paramètres avancés. Dans celui-ci, vous pouvez activer le message de test statique, ainsi que régler l'intervalle.

6. Généralités, maintenance et remarques

6.1. Configuration de la centrale

Sous l'option Configuration de la centrale, vous trouverez, d'une part, toutes les informations importantes concernant votre centrale et pourrez, d'autre part, effectuer les réglages importants du système

Une fois dans l'option Configuration de la centrale, vous verrez les informations suivantes :

- Nom de la centrale (champ de saisie)
- Symbole (peut être remplacé par une photo propre)
- Réseau (affichage du type de connexion réseau)
- Statut de la téléphonie mobile (liste déroulante)
  - Type de module (puce de téléphonie mobile intégrée)
  - Carte SIM (insertion indiquée)
  - Appel téléphonique (indique si l'appel est possible avec la carte SIM insérée)
  - Connexion (affichage de l'état de la connexion)
  - Puissance du signal (dBm)
- Alimentation électrique (affichage bloc d'alimentation ou batterie)
- Logiciel (cliquer dessus pour consulter la version et les notes de publication)
- Module radio (affichage du logiciel du module radio)
- Référence

La roue dentée située en haut à droite permet d'ouvrir d'autres menus de paramètres. Les paramètres relatifs à SIA DC-09, aux appels téléphoniques et au module de téléphonie mobile se trouvent au point 5. Communication.

6.1.1. Informations générales

Sous « Mémoire » sont affichées les informations relatives au support de stockage inséré (disque dur ou carte SD).

Sous « Date et heure » sont affichés le fuseau horaire utilisé et le serveur NTP.

Vous pouvez redémarrer l'installation à l'aide du bouton « Redémarrer ».

6.1.2. Réseau

Ce menu vous permet de consulter les paramètres réseau et de les adapter si nécessaire.

Vous avez le choix entre trois méthodes :
DHCP (par défaut) : Dynamic Host Configuration Protocol est un protocole client/serveur grâce auquel le système Comfion reçoit automatiquement son adresse IP et d'autres informations connexes du routeur.

PPPoE : Point-to-Point Protocol over Ethernet est un protocole réseau qui fournit une connexion directe au sein du réseau interne. Il requiert une authentification par nom d'utilisateur et mot de passe.

Statique : Si vous choisissez « statique », les données réseau du système Comfion sont attribuées manuellement. Consultez à ce sujet l'opérateur du réseau et n'attribuez pas d'adresse IP issue de DHCP.

Remarque	Des paramètres IP incorrects empêchent votre système de se connecter au réseau, ce qui le rend également inaccessible via l'application. Dans ce cas, appuyez sur le bouton « connect » situé à l'arrière de l'appareil pendant 6 secondes, puis relâchez-le. La centrale redémarre alors et réinitialise ses paramètres réseau pour rétablir les paramètres DHCP par défaut.

6.1.3. Paramètres de sécuritié

Mode maintenance	marche/arrêt (par défaut OFF)	Le mode maintenance sert à l'installation et à l'entretien du système. Pendant que le mode maintenance est actif, le système ne peut pas déclencher d'alarme.
Verrouillage de la zone	3x-20x (5x par défaut)	Si une zone se déclenche plus souvent que prévu, cette zone ne se déclenchera plus jusqu'à ce que les alarmes soient effacées de l'historique des alarmes.
Nombre max. de répétitions de la saisie au clavier	3x-20x (5x par défaut)	Indique le nombre de saisies de code PIN erronées sur l'élément de commande, après quoi celui-ci est bloqué.
Time-out de l'unité de commande	5-180 sec (par défaut 30 sec)	Réglage du temps pendant lequel l'élément de commande est bloqué après X saisies erronées
Temporisation d'entrée	5-45 sec (par défaut 10 sec)	Dans le cas d'une installation armée, la temporisation d'entrée est déclenchée par une zone d'entrée ou d'entrée/sortie.
Délai de sortie	5-45 sec (par défaut 30 sec)	Temps avant que la centrale ne passe à l'état armé
Délai de transmission	5-180 sec (par défaut 60 sec)	Si cette propriété est activée dans la zone, la transmission d'un déclenchement est retardée de la durée définie.
Délai panne de courant	0-30 min (par défaut 0 min)	Retard réglable de la signalisation d'une perte de tension (12V DC)
Activer la sirène d'intrusion	marche/arrêt (par défaut AN)	Commande de la sirène en cas d'alarme anti-intrusion
Durée de la sirène de l'alarme d'intrusion	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Activer la sirène anti-sabotage	marche/arrêt (par défaut AN)	Commande de la sirène en cas d'alarme de sabotage
Durée de la sirène de sabotage	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Activer la sirène de l'alarme de panique	marche/arrêt (par défaut OFF)	Commande de la sirène en cas d'alarme agression
Durée de la sirène de l'alarme de panique	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Activer la sirène de l'alarme dégâts des eaux	marche/arrêt (par défaut AN)	Commande de la sirène en cas d'alarme-eau
Durée de la sirène de l'alarme dégâts des eaux	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Activer la sirène d'incendie	marche/arrêt (par défaut AN)	Commande de la sirène en cas d'alarme incendie
Durée de la sirène de l'alarme incendie	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Activer la sirène SOS	marche/arrêt (par défaut OFF)	Commande de la sirène en cas d'alarme d'agression déclenchée via l'application
Durée de la sirène SOS	5-180 sec (par défaut 60 sec)	Durée de la signalisation acoustique par les sirènes intégrées au système
Masquer les erreurs de réseau	marche/arrêt (par défaut OFF)	Détection et signalement d'une erreur de réseau
Masquer les erreurs de batterie	marche/arrêt (par défaut OFF)	Détection et signalement d'une défaillance de la batterie
Masquer la perte de courant	marche/arrêt (par défaut OFF)	Détection et signalisation d'une perte de courant (12V DC)
Masquer le sabotage du couvercle à droite	marche/arrêt (par défaut OFF)	Détection et signalement d'un sabotage du couvercle droit (disque dur)
Masquer le sabotage du couvercle à gauche	marche/arrêt (par défaut OFF)	Détection et signalement d'un sabotage du couvercle gauche (batterie)

6.1.4.Centrale de sauvegarde

Remarque	Pour des raisons de sécurité, le fichier de sauvegarde de votre centrale est entièrement crypté et stocké dans le cloud d'Abus, exclusivement sur des serveurs européens.

Créer une sauvegarde
Sous l'option de menu Sauvegarde sous la configuration de la centrale, vous pouvez créer une sauvegarde manuellement et activer la sauvegarde automatique. La sauvegarde automatique est effectuée chaque semaine.

Importer une sauvegarde
Pour importer la sauvegarde dans une nouvelle centrale, veuillez procéder comme suit :

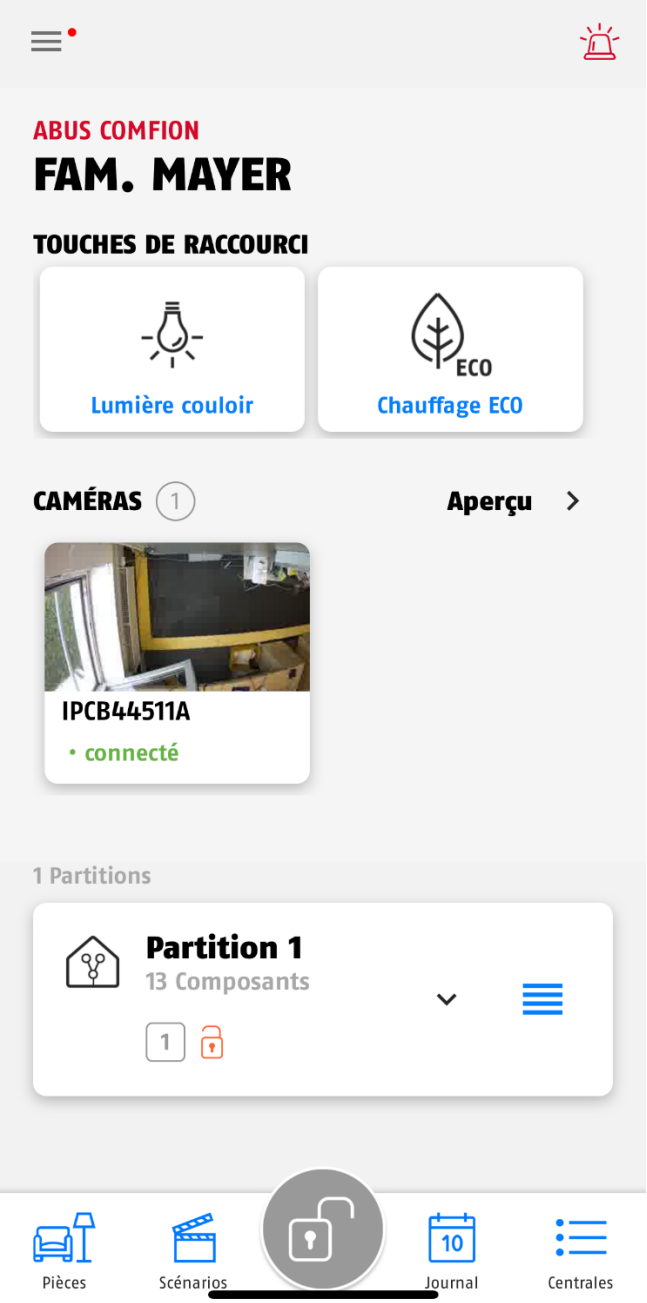
1. Si ce n'est pas déjà fait, déconnectez la centrale d'où provient la sauvegarde du réseau et mettez-la hors tension.
2. Dans l'aperçu des centrales de l'application, cliquez sur le symbole + pour ajouter une nouvelle centrale.
3. Sélectionnez « Importer une sauvegarde ».
4. Scannez le code QR au dos de votre nouvelle centrale.
5. Sélectionnez la centrale à partir de laquelle vous souhaitez charger la sauvegarde.
   Remarque : après l'importation, la sauvegarde est supprimée du cloud et les composants ne fonctionnent plus sur l'ancienne centrale.
6. Saisissez le nom de centrale souhaité pour votre nouvelle centrale.
7. Après confirmation, un code de vérification est envoyé à l'adresse e-mail du propriétaire de la centrale. Saisissez ce code dans l'application et cliquez sur « Démarrer l'importation ».
8. L'importation est maintenant effectuée. Vous pouvez maintenant fermer votre app et attendre de recevoir le message push indiquant que la centrale est en ligne et que l'alimentation électrique est disponible.

Pour restaurer une configuration sur le même matériel (centrale), veuillez procéder comme suit :

1. Réinitialisez la centrale concernée aux paramètres d'usine (appuyez sur le bouton de réinitialisation pendant 10 secondes -> voir 6.5.1)
2. Dans l'aperçu des centrales dans l'app, allez sur le symbole + pour ajouter une nouvelle centrale.
3. Sélectionnez « Restauration ».
4. Scannez le code QR au dos de votre centrale.
5. Saisissez le nom de centrale souhaité pour votre centrale
6. L'importation est maintenant effectuée. Vous pouvez maintenant fermer votre app et attendre de recevoir le message push indiquant que la centrale est en ligne et que l'alimentation électrique est disponible.

6.2. Tableau de bord

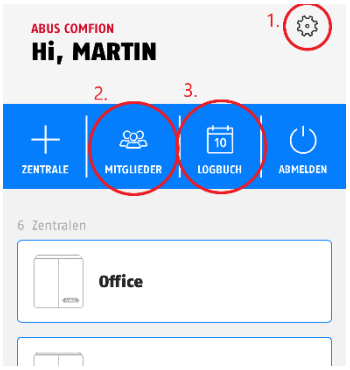
Le tableau de bord vous permet de contrôler l'installation et, même en tant qu'installateur, d'effectuer une grande partie de vos travaux.



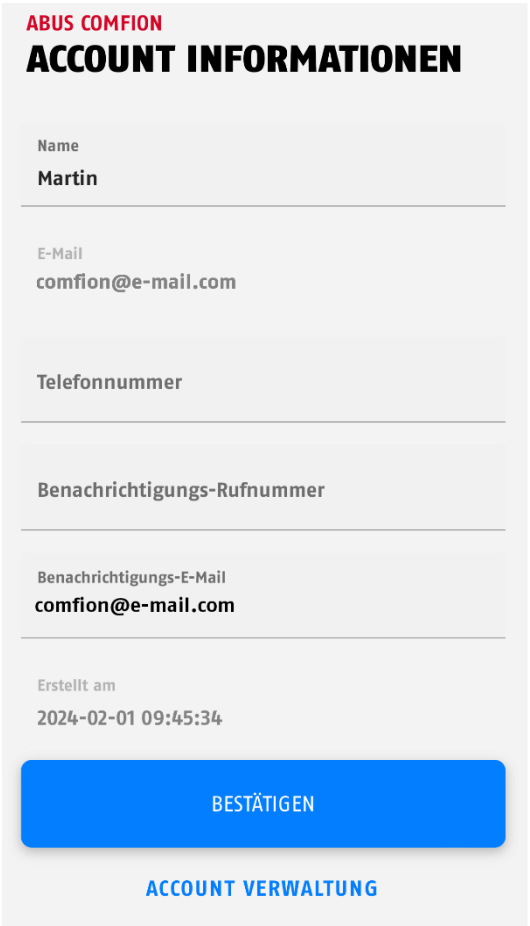
- ➔ Appel de menu & bouton de panique
- ➔ Nom des centrales
- ➔ Touches de raccourci - peuvent être définies dans « Scènes »
- ➔ Aperçu de la caméra - accès aux flux en direct de la caméra et aux paramètres généraux de la caméra
- ➔ Sélection de la caméra - Un clic sur la caméra permet d'ouvrir directement son flux en direct
- ➔ Affichage de la partition. Un long clic permet de modifier la partition. Un bref clic permet d'ouvrir la partition et d'afficher les composants attribués
- ➔ Pièces = Affichage de la vue d'ensemble des pièces & des composants
- ➔ Scénarios = Scènes & Automations
- ➔ Journal = Affichage de la mémoire d'événements
- ➔ Centrales = Aperçu des centrales

6.3. Aperçu de la centrale

L'aperçu de la centrale de l'installation vous permet, outre l'ajout de nouvelles centrales, de voir les centrales existantes et d'y accéder, de modifier les informations de votre compte (1), de gérer vos membres (2) et de consulter le journal du compte (3).



6.3.1. Informations sur le compte



- ➔ Nom du compte (affiché dans la centrale et le journal)
- ➔ E-mail du compte
- ➔ Numéro de téléphone
- ➔ Numéro de téléphone de notification pour les SMS et appels
- ➔ E-mail de notification pour l'envoi d'e-mails par la centrale
- ➔ Date de création du compte
- ➔ Bouton de confirmation permettant l'enregistrement des données
- ➔ Fonction de suppression du compte ABUS interne à l'application

6.3.2. Membres

L'application Comfion vous donne la possibilité de dresser une liste des membres. Cette action est purement facultative et n'est en rien nécessaire au fonctionnement des systèmes Comfion. La liste des membres vous permet de sélectionner facilement les membres lorsque vous ajoutez/invitez de nouveaux utilisateurs à (rejoindre) une centrale.

6.3.3. Journal du compte

Le journal du compte répertorie tous les messages provenant des installations avec autorisation d'accès. Si l'accès à une centrale est bloqué, les entrées du journal de la centrale concernée ne sont pas enregistrées dans le journal du compte.

6.4. Automations & scènes

Le système Comfion vous offre la possibilité de configurer jusqu'à 100 scénarios. Ces scènes, ou automations, sont librement configurables. Vous profitez ainsi d'une flexibilité maximale.

L'onglet « Scènes » vous permet d'ajouter aussi bien des scènes que des automations.

Attention	Il est interdit de créer des automatisations qui se contredisent ou qui forment une boucle d'activation en elles. Une telle situation peut entraîner de graves problèmes de fonctionnement de la centrale.

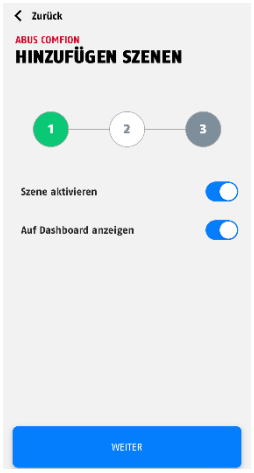
Remarque	Veillez à respecter un intervalle d'au moins 5 secondes entre deux commandes de commutation pour un même appareil, afin de garantir le bon fonctionnement du système.

Scène = action déclenchée par un utilisateur via l'application (touches de raccourci). Possibilité d'affichage dans le tableau de bord. Exemple : Prise ON/OFF via l'application

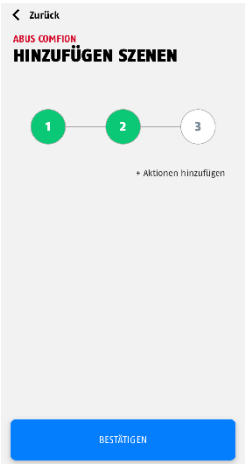
Exemple de configuration d'une scène :

Attribution de noms / symboles

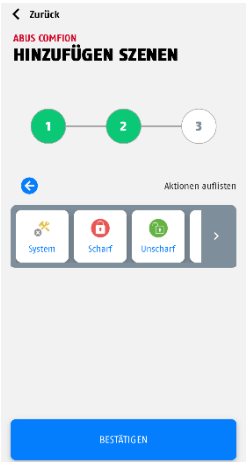
Paramètres de la scène



Ajouter action



Sélection action



Automation = Se compose toujours d'une partie « si » (condition) et d'une partie « alors » (conséquence). Librement configurable.
Exemple : Si l'installation est armée, alors la lumière est éteinte

La partie « si » permet de choisir entre une combinaison « ET » et une combinaison « OU ». Dans le cas d'une combinaison ET, TOUTES les conditions doivent être remplies pour que l'action soit exécutée. Dans le cas d'une combinaison OU, au moins UNE condition doit être remplie pour que l'action soit exécutée.

La partie « si » permet de choisir, pour les événements, entre les catégories suivantes :

- Système -> Vous trouverez ici les événements du système, par ex. une panne de courant, mais aussi l'horaire
- Partition -> Vous trouverez ici les événements de partition, par ex. armée/désarmée, intrusion, prêt pour l'armement, etc
- Zone -> Vous trouverez ici tous les événements liés à la zone (par ex. intrusion zone)
- Pièce -> Vous trouverez ici tous les composants et événements qui y sont liés (p. ex. détecteur d'ouverture, contact ouvert ou commutateur mural actionné)

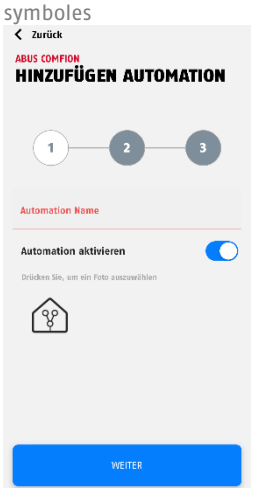
- Explication relative à « Avancé » :
  La section « Avancé » permet de régler une durée pendant laquelle les conditions réglées doivent être satisfaites avant que l'action concernée ne soit exécutée. L'action ne sera exécutée que si les conditions ne changent pas et sont satisfaites pendant la période de temps définie.
  Exemple : Si la porte est ouverte pendant 30 secondes, Alors une notification push est envoyée

La partie Alors distingue :

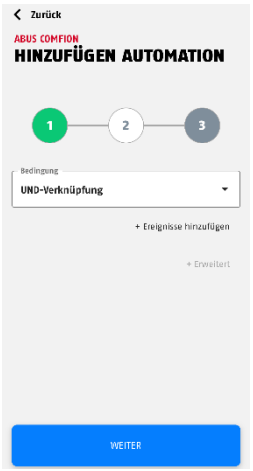
- « Si, alors » -> l'action est exécutée si les conditions définies dans la partie Si sont remplies
- « Si terminé, alors » -> l'action est exécutée lorsque les conditions définies dans la partie Si ne sont PLUS remplies

Exemple de configuration d'une automation :

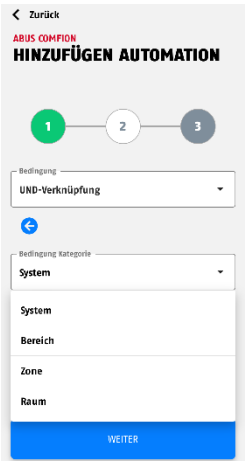
Attribution de noms / symboles



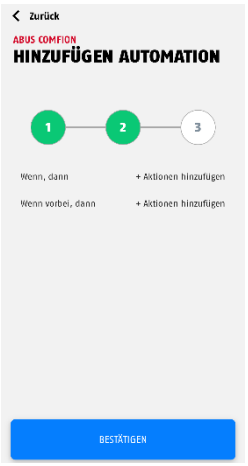
Partie Si



Sélection de la catégorie



Partie Alors



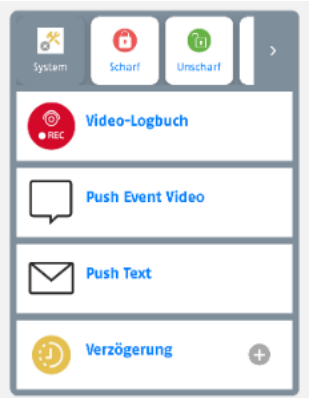
Lorsque vous sélectionnez « Système » dans la partie Alors des scènes ou des automations, les actions suivantes sont disponibles à la sélection :

Journal vidéo : Création d'une entrée dans le journal (15 sec) avec un extrait de l'enregistrement caméra.

Vidéo Évènements Push : Envoi d'une notification push avec un texte définissable et un extrait (15 sec) de l'enregistrement caméra.

Texte push : Envoi d'une notification push avec un texte définissable.

Délai : Délai réglable en secondes - par ex. entre deux actions



6.5. Réinitialisations

6.5.1. Réinitialisation d'usine

Pour réinitialiser l'installation aux paramètres d'usine, maintenez le bouton de réinitialisation (voir 2.3 Description de l'appareil) enfoncé pendant >10 secondes et relâchez-le. Les LED de la centrale s'éteindront après quelques secondes et l'installation effectuera un redémarrage. Après le redémarrage, la centrale se trouve sur les réglages d'usine et peut être configurée à nouveau.

6.5.2. Réinitialisation de l'utilisateur

Pour réinitialiser les utilisateurs de la centrale ou supprimer tous les utilisateurs de la centrale, appuyez 5 fois sur le contact de sabotage gauche (au-dessus du bouton de réinitialisation) en l'espace de 5 secondes. Après quelques secondes, la LED Internet passe brièvement au rouge. Vous devriez recevoir un message push sur les appareils connectés vous informant que la centrale concernée a été supprimée.

Lorsque toutes les LED sont à nouveau vertes (la LED Internet peut clignoter en vert), vous pouvez ajouter à nouveau la centrale via le symbole + dans votre application.

6.5.3. Réinitialisation du réseau

Si vous ne pouvez plus accéder à votre installation sur le réseau en raison d'un mauvais réglage IP, il est possible de réinitialiser la centrale sur DHCP. Pour ce faire, maintenez le bouton de réinitialisation du réseau situé au dos de la centrale (décrit par « Connect ») enfoncé pendant 6 secondes. Après quelques minutes, la centrale devrait être à nouveau accessible.

6.6. Fonctionnement des LED

Remarque	Les témoins LED ci-dessous ne sont n'interviennent qu'après la première mise en service de l'installation

LED alimentation : Indique l'état de la tension et peut signaler des erreurs

Couleur	Signification
Vert	Tension du bloc d'alimentation
Rouge	Fonctionnement sur batterie
Orange	Mise à jour du logiciel

LED Internet (globe) : Indique le statut de la connexion au cloud

Couleur	Signification
Vert	Connecté au cloud (Le propriétaire est créé)
Rouge	Échec de la connexion au cloud
Clignotement vert	Connecté au cloud (Aucun propriétaire créé)

LED réseau (flèches) : Indique la voie de communication actuellement utilisée

Couleur	Signification
Vert	Connecté à Internet par LAN
Rouge	Connexion 3G/4G

LED statut (cadenas) : Indique le statut de l'installation

Couleur	Signification
Rouge	Système armé
Orange	Système partiellement armé
Vert	Système désarmé
Clignotement vert	La centrale se connecte au composant

6.7. Utilisation

6.7.1. Armement / Désarmement

- APP : L'armement/désarmement peut être effectué dans l'app en exécutant les modes d'alarme. Pour ce faire, cliquez dans le tableau de bord sur le bouton central en bas de l'écran (symbole du cadenas) et sélectionnez ensuite l'action (par ex. armement total).
- ÉLÉMENT DE COMMANDE : vous pouvez armer et désarmer le système à l'aide d'un élément de commande sans fil. Pour ce faire, saisissez votre code utilisateur et cliquez ensuite sur la surface d'action à exécuter (touches de verrouillage). Vous trouverez des informations plus détaillées dans le guide de l'utilisateur ou dans le mode d'emploi de l'élément de commande.
- TÉLÉCOMMANDE : vous pouvez attribuer les modes d'alarme aux touches de votre télécommande sans fil et ainsi exécuter l'action correspondante en appuyant sur une touche. Vous trouverez le réglage sous la télécommande.
- AUTOMATION : grâce à une automatisation, vous pouvez lier l'armement ou le désarmement de l'installation à des conditions. Cela permet par exemple d'activer l'armement selon un horaire ou en cas d'activation d'une entrée filaire.

6.7.2. Réinitialisation des alarmes

Le système Comfion doit être réinitialisé par l'utilisateur après une alarme (intrusion, sabotage, etc.) :

- Le système Comfion effectue automatiquement la réinitialisation de l'alarme lors de sa désactivation. Dès que tous les détecteurs déclenchés reviennent à la normale, l'aperçu des alertes disparaît du tableau de bord.

6.8. Explication des symboles

	Composant déclenché (par ex. fenêtre ouverte)
	Sabotage (par ex. boîtier du détecteur ouvert)
	Composant activé (p. ex. son de sirène déclenché)
	État des composants OFF (par ex. prise radio éteinte)
	État des composants ON (par ex. prise radio allumée)
	Mouvement détecté
	Caméra PIR : 1 Créer une photo (bouton de déclenchement) 2 Enregistrement en cours 3 Enregistrement en cours de transfert
	Rupture de câble (par ex. détecteur 3en1)
	Alimentation connectée
	Connexion radio interrompue
	Zone fermée
	Zone ouverte
	Niveau de charge de la pile
	4 barres = excellent 3 barres = très bon 2 barres = bien 1 barre = OK 0 barre = mauvais

6.9. Cloud ABUS

Lors de la première mise en service, le système de sécurité sans fil Comfion se connecte à l'Abus Cloud. L'installation est en outre enregistrée dans le compte d'installateur spécialisé Abus Cloud de l'installateur. Si cela n'est pas souhaité, il est possible de décocher la case « Installateur principal » sous l'utilisateur concerné dans l'installation ou de l'activer chez un autre installateur.

6.10. Remarques concernant le disque dur

- Les vis de fixation du disque dur ne peuvent être serrées qu'à la main
- L'autonomie de la centrale dépend entre autres du disque dur intégré et de sa consommation d'énergie, ainsi que du nombre de caméras et du type d'enregistrement choisi (enregistrement continu, etc.).
- Le disque dur installé dans le système Comfion doit présenter le format exFAT ou NTFS
- Ne remplacez le disque dur que lorsque la centrale est hors tension

6.11. Maintenance et entretien par l'installateur

Lors de la maintenance routinière, testez le bon fonctionnement du système :

- Vérifiez si le système Comfion ne présente pas de signes manifestes de dommages au niveau du boîtier ou des caches avant.
- Contrôlez le fonctionnement des interrupteurs anti-sabotage (arrachement du mur/couvercle du boîtier à gauche, couvercle du boîtier à droite)
- Contrôlez l'état des batteries de secours
- Nettoyez le boîtier
    - En guise de nettoyage, il convient d'essuyer la surface avec un chiffon sec et doux.
    - N'utilisez pas d'eau, de solvants ou de détergents.
- Contrôlez l'intensité du signal et l'état des piles/de la batterie de tous les composants
- Remplacez les piles ou les batteries en suivant les instructions du fabricant
- Testez chaque composant.
- Nettoyez avec précaution les lentilles de tous les détecteurs PIR et de toutes les caméras à l'aide d'un chiffon propre, sec et doux.
    - N'utilisez pas d'eau, de solvants ou de détergents.
- Contrôlez le fonctionnement de tous les détecteurs.
- Testez tous les émetteurs de signaux
- Testez la communication.

Remarque	ABUS recommande de changer la batterie centrale après 3 ans maximum. En cas de durée de fonctionnement plus longue, une chute soudaine des performances ne peut pas être exclue.

Comment changer la batterie de la centrale :

- Basculez la centrale en mode maintenance (paramètres de sécurité)
- Ouvrez le couvercle gauche du boîtier
- Débranchez l'alimentation électrique ainsi que l'ancienne batterie de la centrale
- Attendez 30 secondes
- Branchez la nouvelle batterie et rebranchez l'alimentation électrique
- Fermez le couvercle de l'installation et quittez ensuite le mode maintenance

6.12. Tableau des intensités de signal radio

Le tableau suivant décrit la signification des valeurs de signal des composants radio Comfion affichées en dBm.

Valeur-RSSI (dBm)	Signification	Affichage sur le composant
<= -100	Faible	0 Barre
<= -96	D'accord	1 Barre
<= -91	Bon	2 Barres
<= -86	Très bon	3 Barres
> -86	Excellent	4 Barres

7. Historique des versions

7.1. Aperçu

Date de publication	Version du firmware de la centrale	Version App IOS/Android
21.03.2024	1.0.4736	0.2.1360
26.03.2024	1.0.4751	inchangé
10.05.2024	1.0.4957	0.3.1401
02.07.2024	1.0.5150	0.5.1471
16.09.2024	1.0.5398	0.5.1575 / 0.5.1577
11.11.2024	1.0.5500	0.6.1626
15.11.2024	1.0.5510	Inchangé
18.02.2025	1.0.5727	0.6.1702
28.02.2025	1.0.5782	Inchangé
18.03.2025	1.0.5836	Inchangé

7.2. Notes de publication

Vous trouverez les notes de publication de la mise à jour actuelle du firmware dans votre Comfion App ou sous le lien suivant :
https://l.ead.me/becYdV

8. Garantie

- Les produits ABUS sont conçus, fabriqués et testés avec le plus grand soin et dans le respect des réglementations en vigueur.
- La garantie s'applique exclusivement aux défauts dus à la présence de vices de matériel ou de fabrication au moment de la vente. Si la présence d'un défaut de matériel ou de fabrication est prouvée, le module sera réparé ou remplacé, à la discrétion du garant.
- Dans un tel cas, la garantie s'éteint à l'expiration de la période de garantie initiale de 2 ans. Toute autre réclamation est expressément exclue.
- ABUS n'est pas responsable des défauts et dommages dus à des facteurs extérieurs (par ex. transport, force, erreur de manipulation), à une utilisation non conforme, à l'usure normale ou au non-respect du présent manuel et des consignes d'entretien.
- Pour revendiquer un droit à la garantie, il convient de joindre au produit concerné la preuve d'achat originale portant la date d'achat et une brève description écrite du défaut.
- Si vous constatez, au niveau du produit, un défaut qui était déjà présent au moment de la vente, veuillez vous adresser directement à votre revendeur au cours des deux premières années.

9. Instructions relatives à l'élimination

Éliminez l'appareil conformément à la directive européenne relative aux déchets d'équipements électriques et électroniques 2012/19/UE - DEEE. Pour toute question, veuillez vous adresser aux autorités communales responsables de l'élimination des déchets. Vous pouvez obtenir des informations sur les points de collecte de vos appareils usagés auprès de l'administration communale ou de votre ville, des entreprises locales de collecte des déchets ou de votre revendeur, par exemple.

10. Conformité

10.1. Déclaration de conformité UE

Par la présente, ABUS Security Center GmbH & Co. KG certifie que le type d'installation radio FUAA80000 est conforme aux directives 2014/53/UE et 2011/65/UE. La déclaration de conformité UE est disponible dans son intégralité à l'adresse Internet suivante : abus.com > Recherche d'articles > FUAA80000 > Téléchargements

10.2. Conformité à la norme EN 50131

Le système de sécurité FUAA80000 est certifié conforme au degré de sécurité 2 lorsqu'il est correctement installé, conformément aux normes EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 et EN 50131-5-3:2017.

ABUS I Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tél: +49 82 07 959 90-0

ABUS
Security Tech Germany

FUAA80000

INSTALLATIEHANDLEIDING

Comfion draadloos beveiligingssysteem

V2.0

1. Algemeen

1.1. Inleiding

Hartelijk dank dat u hebt gekozen voor het **draadloze beveiligingssysteem Comfion** , een product van ABUS Security Center (ook wel kort "ABUS" genoemd).

Deze handleiding bevat belangrijke beschrijvingen, technische gegevens, overzichten en verdere informatie over projectplanning, inbedrijfstelling en bediening van het **draadloze beveiligingssysteem Comfion**.

De hier beschreven producten/systemen mogen alleen worden geïnstalleerd en onderhouden door personen die gekwalificeerd zijn voor de betreffende taak. Gekwalificeerd personeel voor de installatie en het onderhoud van het systeem houdt in de regel een geschoolde, deskundige ABUS-partner in.

1.2. Beoogd gebruik / Wettelijk verplichte aanwijzingen

De verantwoordelijkheid voor het wettelijk conforme gebruik van het product ligt bij de koper of klant en de eindgebruiker. In overeenstemming met de aansprakelijkheid van de fabrikant voor zijn producten zoals gedefinieerd in de productaansprakelijkheidswetgeving, moet de bovenstaande informatie in acht worden genomen en worden doorgegeven aan exploitanten en gebruikers. Niet-naleving ontslaat ABUS Security Center van zijn wettelijke aansprakelijkheid.

Oneigenlijk of ongebruikelijk gebruik, reparatiewerkzaamheden of wijzigingen die niet uitdrukkelijk door ABUS zijn goedgekeurd, en ondeskundig onderhoud kunnen leiden tot storingen en moeten worden vermeden. Wijzigingen die niet uitdrukkelijk door ABUS zijn toegestaan, leiden tot het verlies van aansprakelijkheid, garantie en speciaal overeengekomen garantie-aanspraken.

Architecten, technische gebouwplanners (TGA) en andere adviserende instellingen zijn verplicht alle benodigde productinformatie bij ABUS op te vragen om te voldoen aan de informatie- en instructieverplichtingen volgens de Wet Productaansprakelijkheid. Gespecialiseerde dealers en installateurs moeten de informatie in de ABUS-documentatie naleven en indien nodig doorgeven aan hun klanten.

Meer informatie is te vinden op www.abus.com op de algemene pagina of voor dealers en installateurs in het partnerportaal op https://www.abus-sc.nl

1.3. Klantenservice

Neem voor verdere hulp contact op met uw leverancier.

Algemene informatie over het **draadloze beveiligingssysteem Comfion** vindt u op onze homepage onder:
https://www.abus.com/nl/product/FUAA80000

1.4. Colofon

Nederlandse editie 05/2024

Met de publicatie van nieuwere montagehandleidingen verliest deze uitgave haar geldigheid.

ABUS Security Center aanvaardt geen aansprakelijkheid voor technische of drukfouten en de gevolgen daarvan. De informatie in deze installatiehandleiding is naar eer en geweten samengesteld, rekening houdend met de huidige stand van de techniek. Zij worden regelmatig herzien en waar nodig bijgewerkt of gecorrigeerd.

1.5. Verklaring van symbolen

In deze installatiehandleiding worden de volgende symbolen gebruikt:

Symbool	Signaalwoord	Betekenis
	Opgelet	Duidt op een risico op letsel of gezondheidsrisico's door elektrische spanning
	Belangrijk	Duidt op mogelijke schade aan het apparaat/de accessoires of een risico op letsel of gevaren voor de gezondheid
	Aanwijzing	Geeft belangrijke informatie aan

2. Werkingsprincipe en eigenschappen

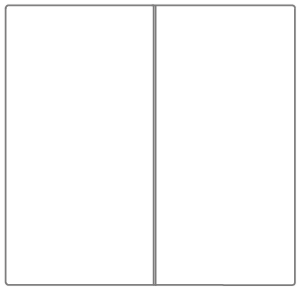
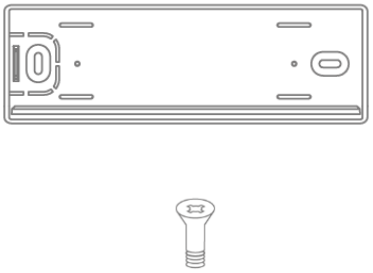
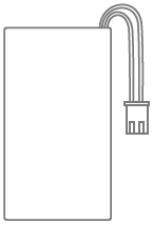
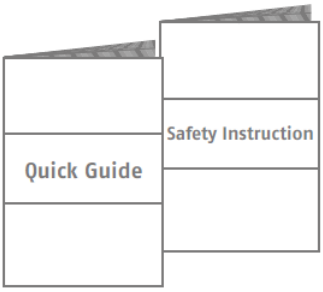
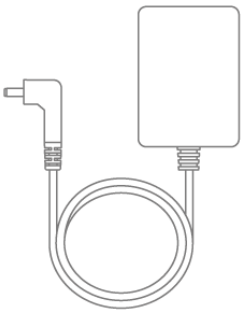
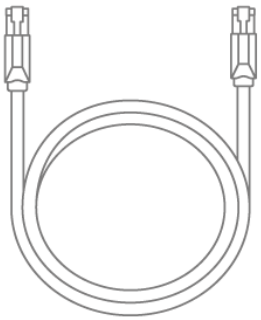
2.1. Productkenmerken

Het **FUAA80000 Comfion draadloze beveiligingssysteem** is een EN-Klasse-2 gecertificeerd beveiligingssysteem met Smart-Home-functies. Het systeem kan worden ingesteld en bediend via de intuïtieve app of het ABUS Cloud-Portal.

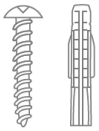
Belangrijkste kenmerken:

- Eenvoudige montage: Dankzij de draadloze technologie kan het systeem op elk gewenst moment en met weinig moeite achteraf worden ingebouwd
- Geïntegreerde NVR: Video-opname met maximaal 4 camera's op optionele HDD en Snapshots op optionele SD-kaart.
- Veilige 868Mhz band met met AES128-bit encryptie: Dit zorgt voor een hoge mate van betrouwbaarheid van de transmissie, terwijl de bidirectionele radio veiligstelt dat het radiosignaal is aangekomen
- Tot 1000 m radiobereik (vrije veld)
- Jamming-bewaking: Als een stoorzender wordt gedetecteerd, laat Comfion een alarm horen
- Veel mogelijkheden in één systeem: 160 apparaten, 50 gebruikers, 40 partities, 100 scenario's
- Veiligheid voor uw klant en de verzekeringsmaatschappij: EN-Grade-2 certificering van alle alarmcomponenten
- Een meldkamer inschakelen: Geïntegreerd meldkamerprotocol (SIA DC-09)
- Voor communicatie & toegang: Geïntegreerde mobiele radiomodule (2G/3G/4G) voor uitvalveilige communicatie, alarmering en toegang op afstand, zelfs zonder internetverbinding op locatie
- Alle informatie altijd bij de hand: Meldingen optioneel via sms, e-mail of pushbericht

2.2. Leveringsomvang

		
1 x centrale	1 x wandhouder & 2x schroeven	1x accu
		
Beknopte handleiding en veiligheidsinstructies	1 x netvoedingsadapter	LAN-kabel

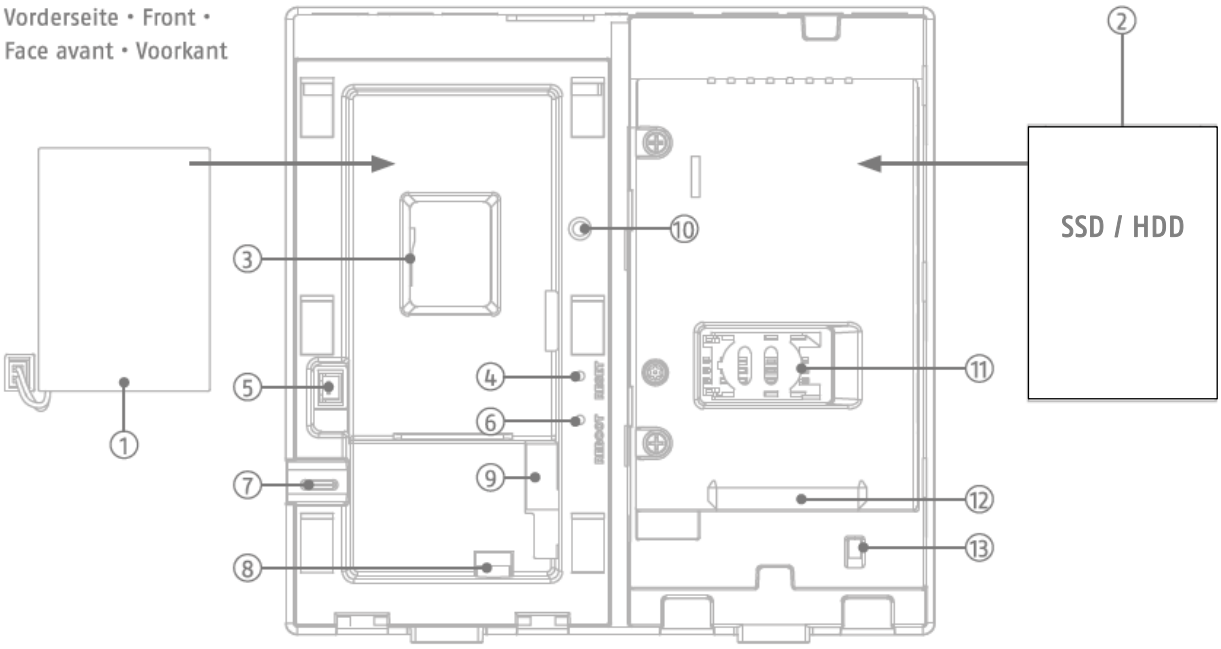
Nodig


2 x schroeven/pluggen Ø 7.0 mm (M4)

2.3. Beschrijving van het apparaat

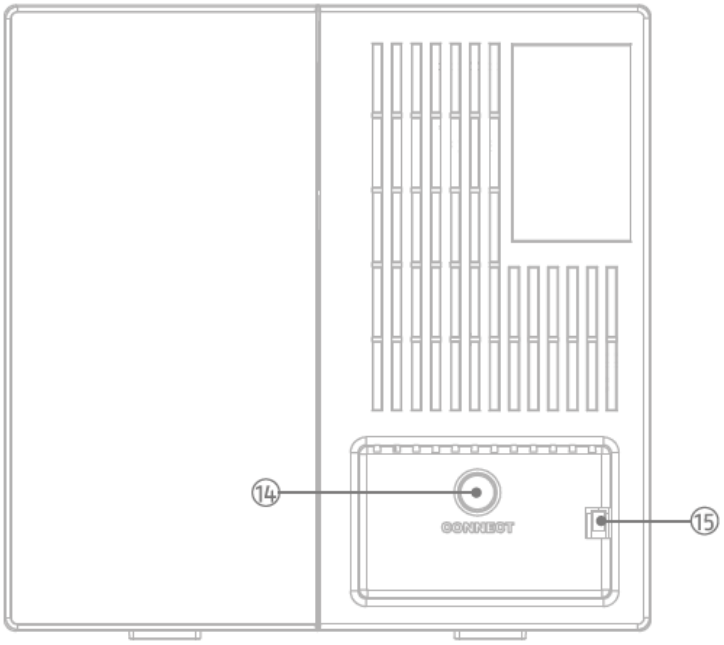
Productopbouw

Vorderseite • Front •
Face avant • Voorkant



1. Noodstroom-accu
2. Harde schijf (niet meegeleverd)
3. MicroSD-kaartsleuf
4. Resettoets
5. Aansluiting voor noodstroomaccu
6. Herstart-toets
7. Kabeldoorvoer
8. Aansluiting externe voeding
9. RJ45-aansluiting
10. Sabotageschakelaar (links)
11. SIM-kaartsleuf (mini-SIM)
12. Aansluiting SATA harde schijf
13. Sabotageschakelaar (rechts)
14. Netwerkreset-toets
15. Sabotageschakelaar (wand)

Rückseite • Back •
Verso • Terug



Oberseite • Top •
En haut • Top

16. Power-LED
- Groen / DC-voeding
- Rood / Batterij
- Geel / Firmware-update

18. Netwerk-LED
- Groen / Ethernet
- Rood / 3G/4G-Netwerk

17. Internet-LED
- Groen / online & Admin geregistreerd
- Rood / offline
- Groen knipperen / online & Admin niet geregistreerd

19. Status-LED
- Rood / ingeschakeld
- Geel / gedeeltelijk ingeschakeld
- Groen / uitgeschakeld
- Groen knipperen / Teach-in procedure radiocomponent

2.4. Technische gegevens

Afmetingen (b x h x d)	165 x 165 x 61 mm
Gewicht	596g (met backup-accu, zonder harde schijf)
Bedrijfstemperatuur	-10 °C tot +40 °C
Milieuklasse	II (EN 50131-1 + A3:2020)
Luchtvochtigheid	max. 85% RL (relatieve luchtvochtigheid)
Aansluitingen	12V DC-aansluiting, RJ45 (LAN), SATA-aansluiting, SIM-slot, micro-SD kaart slot
Indicaties	Status-LED (voeding, internet, netwerk, systeemstatus)
Toetsen	Herstartknop, resetknop
Radiofrequentie / modulatie	868.0 - 868.6 MHz / GFSK
Vermogen RF / bereik	max. 25 mW (14dBm) / 1000m, vrij veld
Aantal draadloze componenten	160
Aantal zones	40
Aantal gebruikers	51
Aantal gebeurtenissen	> 10.000
Communicatie	Netwerkinterface: Ethernet 10/100 Mbps SSL/TLS Mobiel netwerk (back-up): 3G UMTS / 4G LTE SMS & spraak: 2G GSM
Stroomvoorziening	Primair: DC 9V / 2A, secundair: LiPo-accu 7,4V / 2.500mAh
Type voeding	Type A, voeding in overeenstemming met EN50131-1+A3:2020 en EN50131-6+A1:2021
Buffertijd - accubedrijf	> 12 uur volgens EN50131-1+A3:2020 Klasse 2
Sabotagebescherming (detectie / bescherming)	ja (1x wandafbreekcontact; 2 x behuizingscontact)
Supervisietijd	900 - 3600 s (standaardinstelling: 3.600 s)
Veiligheidsklasse	Klasse 2 (EN 50131-1 + A3:2020)
Conformiteit	Veiligheidsklasse 2 bij correcte installatie conform EN 50131-1+A3:2020, EN 50131-3:2009 en EN 50131-5-3:2017
EG-richtlijnen	RED: 2014/53/EU, RoHS: 2011/65/EU + 2015/863 Algemene veiligheid: 2001/95/EG

3. Montage en ingebruikname

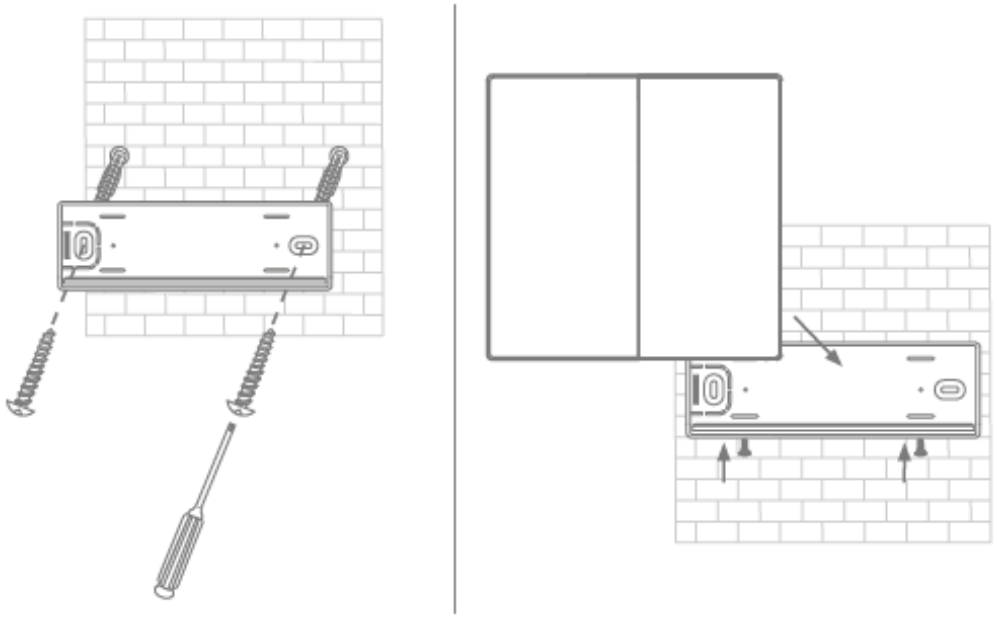
3.1. Wandmontage van de centrale

Aanwijzing	- Monteer de centrale aan de wand op een hoogte van ongeveer 1,5m - Houd aan alle kanten minstens 1 m afstand tot de volgende apparaten aan: Elektrische apparaten, metalen voorwerpen of apparaten met radio-emissies (bijv. routers, magnetrons) - aangezien deze de radioprestaties van het systeem kunnen beïnvloeden.

Bevestig de wandbeugel aan de wand met schroeven en pluggen. (bijvoorbeeld M4)

Plaats de centrale op de wandbeugel en zet deze vast met de voorgemonteerde schroeven.

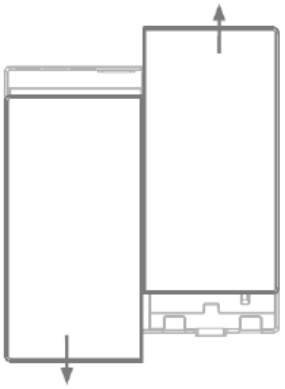
Aanwijzing	Als de centrale van de wandbeugel wordt gehaald en het deksel van de behuizing wordt geopend, wordt er een sabotage-alarm geactiveerd. Voer alleen noodzakelijke werkzaamheden aan de hardware uit als de onderhoudsmodus is geactiveerd (*Centrale-configuratie -> Tandwiel-icoon -> Beveiligingsinstellingen*)



3.2. Inbedrijfstelling van het systeem

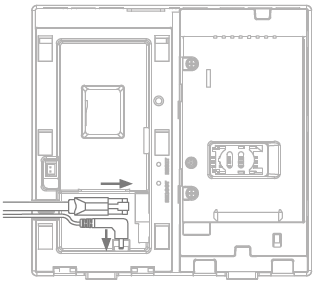
3.2.1. Voorbereiding van de hardware

- Schuif het linker deksel naar beneden en het rechter deksel naar boven om de behuizing te openen.



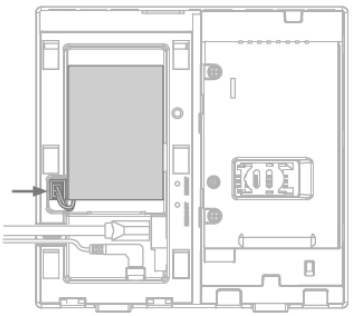
Aanwijzing	Als u een harde schijf, SIM-kaart of SD-kaart wilt gebruiken, plaatst u deze vóór het volgende punt (netspanning toevoegen).

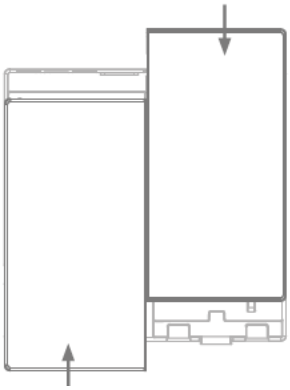
Tip	Formatteer uw SD-kaart of harde schijf in exFAT- of NTFS-formaat voordat u ze plaatst. Plaats of verwijder de SD-kaart of harde schijf nooit als de centrale bezig is met het opstartproces (boot).



- Sluit de Ethernetkabel & netwerkkabel aan op de centrale om de stroom- en netwerkverbinding tot stand te brengen en wacht tot de 4 LED's op de centrale oplichten (dit kan tot 40 seconden duren).

- Sluit de noodstroomaccu aan





- Sluit de behuizing met de twee frontafdekkingen

3.2.2. Instellingen verrichten via app

Aanwijzing	De eerste inbedrijfstelling van de Comfion-centrale en de daarmee gepaard gaande koppeling met het gespecialiseerde partnerportaal en de bijbehorende installateur moet via een app plaatsvinden.

Stap 1:
Download de Comfion-app uit uw app store op uw mobiele apparaat (IOS of Android).

Stap 2:
Volg de instructies in de app tot u bij de inlogpagina komt

Stap 3:
Log in met uw ABUS Single Sign-On gegevens (partnertoegang)
Als u nog geen account hebt, maak dan een (gratis) account aan door op de knop "Registreren" te klikken.

Stap 4:
Na het inloggen ziet u het overzicht van het centrale. Voeg een nieuw centrale toe met de Plus-knop.

Stap 5:
Als u het systeem in bedrijf stelt voor een klant, selecteer dan "Ik ben een installateur". Hiermee wordt u vastgelegd in de rol van installateur. Als u het systeem voor uzelf installeert, selecteer dan "Ik ben een gebruiker". Hierdoor wordt de rol Admin aangemaakt met installateurs- en beheerdersrechten.

Stap 6:
Scan de QR-code op de achterzijde van de centrale.

Aanwijzing	Let erop dat het systeem verbonden is met het internet.

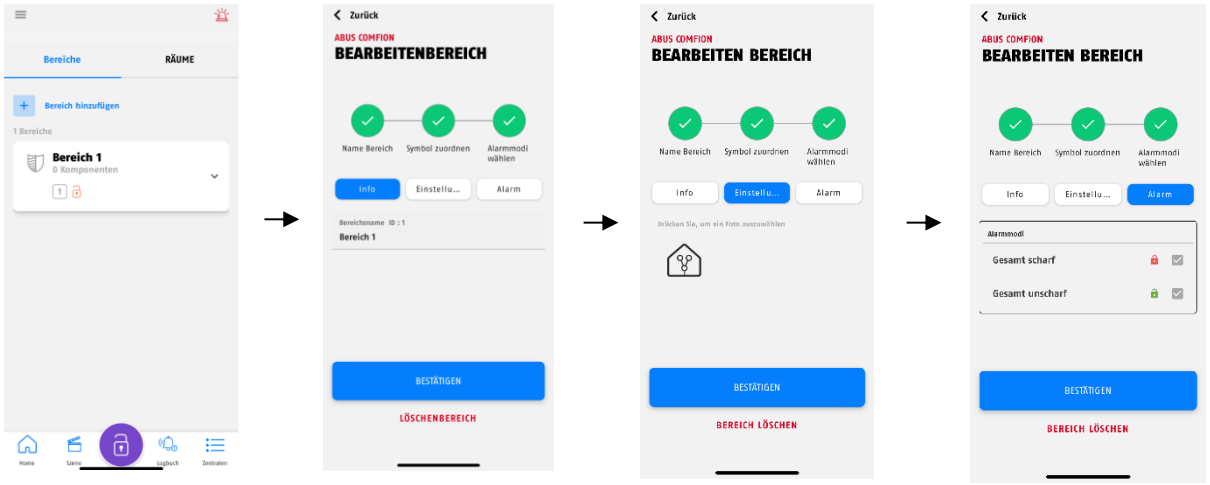
Stap 7:
Wijs een naam voor de centrale toe en bevestig deze. Het systeem zal nu een firmware-update starten voordat u toegang krijgt tot het systeem. De firmware-update kan enkele minuten duren en vereist dat het centrale opnieuw wordt opgestart. De voedings-LED knippert oranje tijdens de update.

Stap 8:
Na het opnieuw opstarten van het centrale wordt het systeem niet langer grijs weergegeven in het centrale-overzicht en kan het worden opgeroepen door erop te klikken.

3.2.3. Partities

Partities bieden u de mogelijkheid om het te bewaken object op te delen en om het gedifferentieerd in en uit te schakelen. In combinatie met de alarmmodi kunt u partities samen of afzonderlijk schakelen.

In de fabriekstoestand heeft het systeem een voorgeconfigureerd partitie. U kunt deze partitie bewerken door deze knop lang ingedrukt te houden.



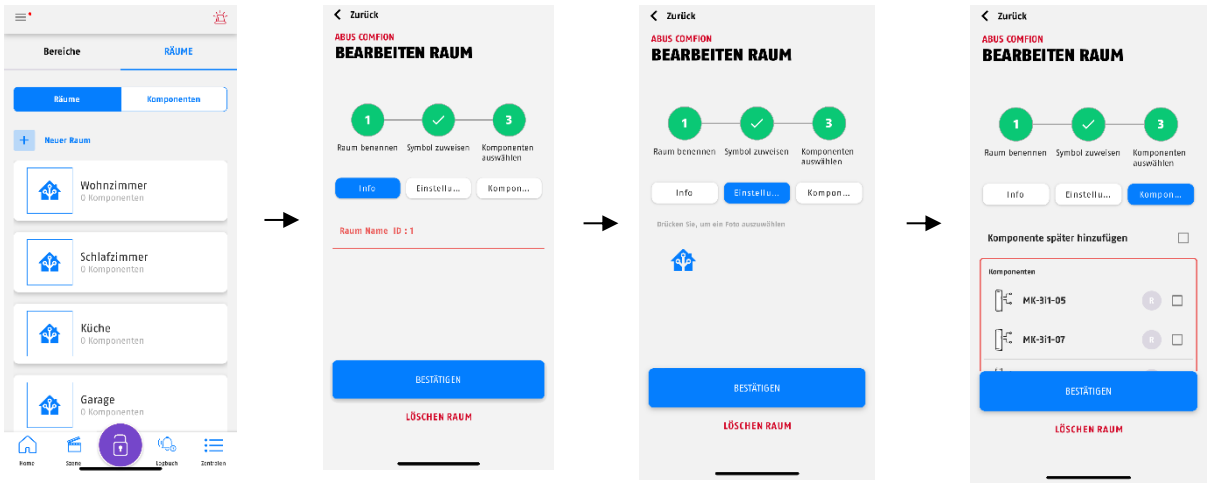
U kunt extra partities aanmaken door op de knop "Nieuwe partitie toevoegen" te klikken.

Met het draadloze beveiligingssysteem Comfion is het aan te raden om de buitenschil en het interieur in afzonderlijke partities te verdelen. Deze kunnen vervolgens naar wens worden ingeschakeld met behulp van de vrij configureerbare alarmmodi.

3.2.4. Ruimtes

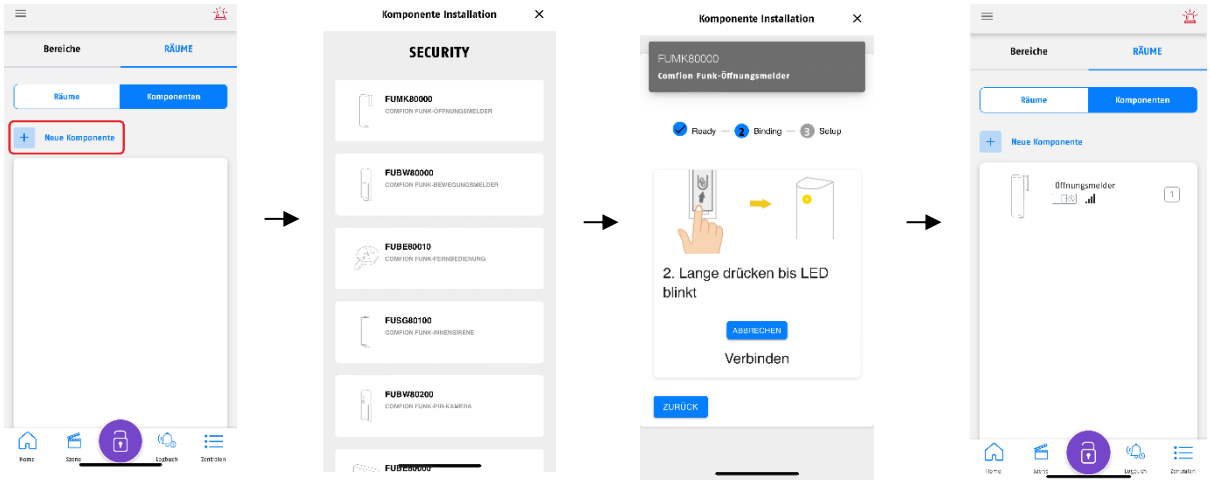
Het Comfion draadloze beveiligingssysteem biedt u de mogelijkheid om uw componenten toe te wijzen aan ruimtes. Dit dient om de identificatie van componenten te vereenvoudigen en heeft geen functionele eigenschappen. Ruimtes zijn niet toegewezen aan partities, wat betekent dat u onderdelen van verschillende partities in één ruimte kunt hebben.

In de fabriekstatus heeft het systeem een aantal vooraf gedefinieerde ruimtes. U kunt deze ruimtes vrij bewerken of helemaal verwijderen. U kunt de ruimte bewerken door deze knop lang ingedrukt te houden.



3.2.5.Componenten

De tab "Ruimtes" op het dashboard brengt u naar het componentenoverzicht, waar u ook de knop "Nieuwe component toevoegen" vindt. U kunt dit gebruiken om uw Comfion-producten aan het systeem toe te voegen.



U kunt met een lange klik ook een component bewerken die al is ingeleerd en de volgende apparaatinstellingen aanpassen:

Tijdelijke deactivering	UIT (standaard): Component functioneert normaal AAN: Component wordt gedeactiveerd (geen functie)
Naam	Toewijzing van een naam aan de component
Zonenummer	Toewijzing van het zonenummer (wordt automatisch gedaan door het systeem)
Zonetype	• Ingang -> *activeert een ingangsvertraging, waarna een inbraakalarm wordt geactiveerd* • Uitgang -> *kan worden geopend tijdens de uitgangsvertraging, functioneert als een directe zone na inschakelen* • Ingang/Uitgang -> *gebruikt een ingangs- en uitgangsvertraging* • Onmiddellijk (inbraak) -> *activeert een inbraakalarm wanneer het systeem is ingeschakeld* • Onmiddellijk (bewaakt) -> *werkt als de Meteen-zone wanneer het systeem is ingeschakeld; wanneer het systeem is uitgeschakeld, wordt een melding verzonden wanneer dit wordt geactiveerd* • 24-uurs inbraakalarm -> *inbraakalarm onafhankelijk van systeemstatus* • 24-uurs wateralarm -> *Wateralarm onafhankelijk van systeemstatus* • 24-uurs brand -> *Brandalarm onafhankelijk van systeemstatus* • Slotbewaking -> *Open zone voorkomt inschakelen maar activeert geen alarm*
Zone gedrag	• Overbruggen mogelijk -> *Als de zone wordt geactiveerd, terwijl deze scherp staat, kunt u deze overbruggen* • Vertraging van transmissie: Als dit item geactiveerd is, wordt de signalering van zone-alarmen vertraagd met de geprogrammeerde tijd.
Activering sirene	• Activeert de sirene

Aanwijzing	Als een melder is geprogrammeerd voor het zonetype uitgang of ingang/uitgang, controleert het systeem de status van de melder pas nadat de vertragingstijd is verstreken bij ingeschakeld systeem. - Als de melder niet gereed is na het verstrijken van de tijd en "met overbruggen" is geactiveerd, wordt de melder automatisch overbrugt na de vertragingstijd en wordt het systeem ingeschakeld. - Als de melder niet gereed is nadat de tijd is verstreken en "met overbruggen" is gedeactiveerd, wordt het systeem niet ingeschakeld.

3.2.6. Alarmmodi

Het draadloze beveiligingssysteem Comfion werkt met zogenaamde "alarmmodi", die de kern van het systeem vormen. Dit zijn in- en uitschakelbare koppelingen tussen partities en gebruikers.

In een alarmmodus bepaalt u welke gebruiker welke partitie daarmee in- of uitschakelt. Dit kan worden gebruikt om alle mogelijke scenario's voor het in- en uitschakelen af te beelden.

In de praktijk voert een gebruiker bij het in- of uitschakelen in werkelijkheid een alarmmodus uit.

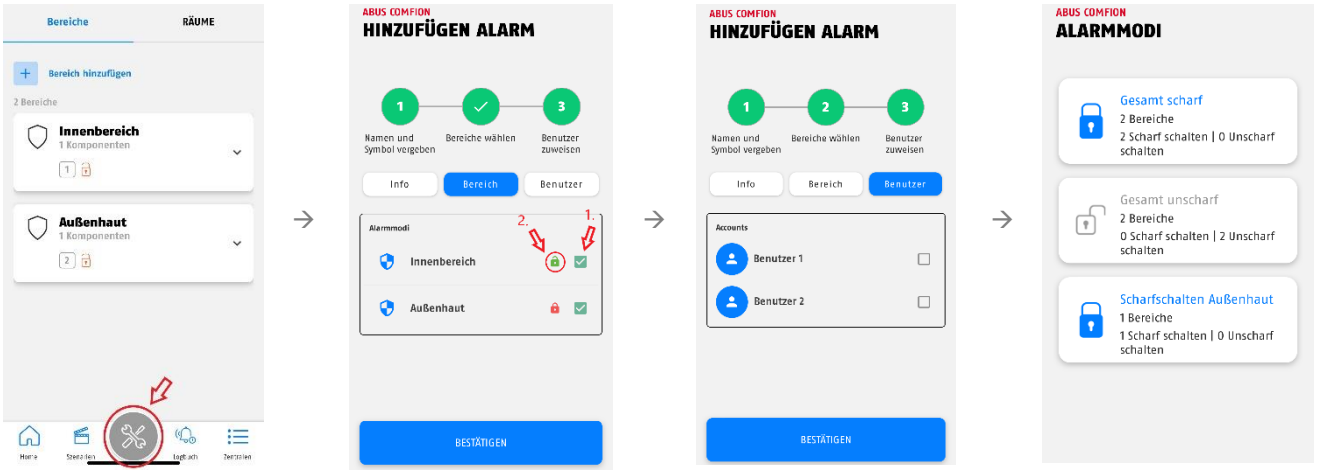
Tip	Het Comfion draadloze beveiligingssysteem heeft twee vooraf geconfigureerde alarmmodi in de fabrieksinstellingen: "Volledig ingeschakeld" en "Volledig uitgeschakeld", die alle gemaakte bereiken bevatten.

Uitvoering van een alarmmodus

- De knop in het midden onderaan het scherm toont de actuele status van het systeem (ingeschakeld, uitgeschakeld, gedeeltelijk ingeschakeld of onderhoudsmodus)
- Door op de knop te drukken, worden de beschikbare alarmmodi weergegeven en kunt u een willekeurige schakelopdracht uitvoeren.

Alarmmodi aanmaken of bewerken

1. U kunt het beheer van de alarmmodi openen door op de knop in het midden onderaan te klikken zoals beschreven in de vorige stap en vervolgens op het Tandwiel-icoon in de rechterbovenhoek van het scherm.
2. Klik vervolgens op "Alarmmodus toevoegen" of bewerk een bestaande alarmmodus door er lang op te drukken.
3. Nadat u de naam voor de alarmmodus hebt toegewezen, selecteert u de partities EN de aard van de schakeling (inschakelen of uitschakelen). Klik op het symbool om de aard van de schakeling te wijzigen.
4. Selecteer in de volgende stap de gebruikers die geautoriseerd moeten worden om deze alarmmodus te schakelen.
5. Na voltooiing verschijnt de alarmmodus in uw overzicht en kunt u deze gebruiken.



3.3. Camera's (NVR)

Met behulp van het ONFIV integratieprotocol kunnen verschillende camera's uit de ABUS Professional Line worden geïntegreerd in het draadloze Comfion beveiligingssysteem. U kunt tot 4 camera's integreren in de Comfion en een snapshotlaten opnemen (SD of HDD) tijdens een gebeurtenis bij ingeschakeld systeem of permanent laten opnemen (24/7) (HDD).

Tip	Er is een harde schijf (HDD) nodig in het centrale voor continue opname.

3.3.1. Integratie van camera's

Het Comfion-systeem zoekt standaard automatisch naar ONFIV-camera's in het netwerk en voegt deze toe aan het systeem. U kunt het Automatisch camera zoeken deactiveren in het camera-overzicht in de camera-instellingen.

Ga als volgt te werk bij het integreren van de camera's:

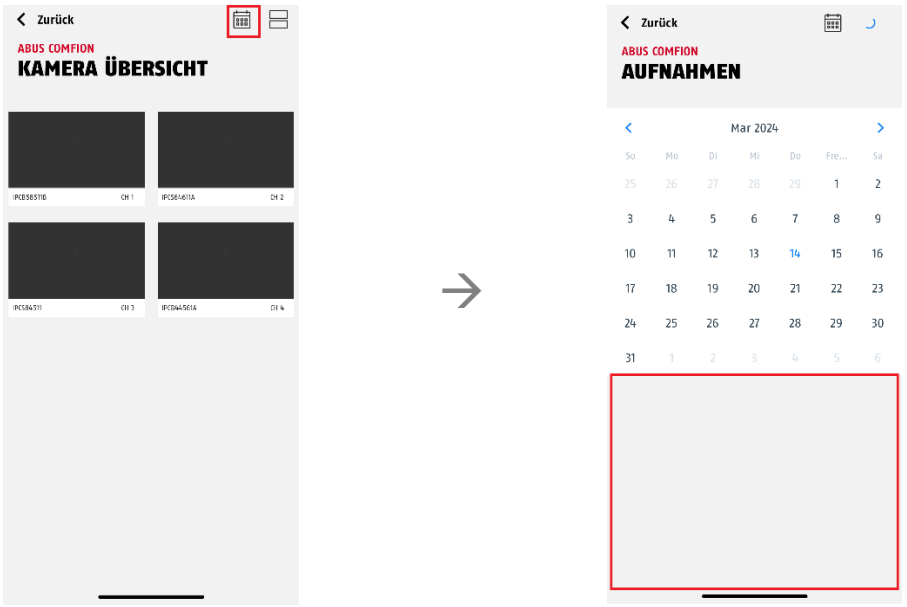
1. Integreer de camera in hetzelfde netwerk als de Comfion.
2. Open de ABUS IP-Installer en activeer de camera.
3. Open de camera-interface, log in als de installateur en open de configuratie.
4. Stel in de geavanceerde netwerkinstellingen onder integratieprotocol ONVIF in, sla deze instelling op en maak een ONFIV-gebruiker aan -> wijs dezelfde gebruikersnaam en hetzelfde wachtwoord toe als een bestaande Admin of installateur bij de camera. (Zorg ervoor dat je minstens ONFIV versie 21.12 hebt)
5. Voer de video-instellingen in de camera uit zoals beschreven in het informatievak hieronder.
6. Sla de ONFIV-gebruikersgegevens op in de Comfion
7. Test de camerafuncties (livebeeld, enz.)

Aanwijzing	De volgende videostream-instellingen worden aanbevolen afhankelijk van het aantal geïntegreerde camera's (kanalen) om een storingsvrije stream te garanderen, zelfs als 4 kanalen tegelijkertijd worden opgeroepen en continu worden opgenomen. Primaire stream: • 1 kanaal: 1080p Resolutie; Bitrate : 4096kbps • 2 kanalen: 1080p Resolutie; Bitrate : 2048kbps • 3 kanalen: Resolutie 1080p; Bitrate : 1024kbps • 4 kanalen: Resolutie 1080p; Bitrate : 1024kbps Secundaire stream: • 1-4 kanalen: Resolutie: 360p; Bitrate 512kbps

Aanwijzing	• De maximale resolutie van 4MP per kanaal mag niet worden overschreden. • De maximale bitrate mag nooit hoger zijn dan 4 x 2048kbps = 8192kbps (alle kanalen bij elkaar opgeteld)

3.3.2. NVR-bediening

Het camera-overzicht brengt u naar de parallelle weergave van alle kanalen. U kunt het livebeeld van alle geïntegreerde camera's hier bekijken. U kunt de kalenderfunctie gebruiken om de bestaande opnamen in het systeem te bekijken, gesorteerd op datum. De Comfion knipt de opnames in clips van 15 minuten.



Door op de betreffende camerastream te klikken, kunt u het beeld in groot formaat weergeven en krijgt u toegang tot de specifieke functies van de camera (bijv. PTZ, 2WayAudio, enz.).

4. Gebruikers en autorisatiegroepen

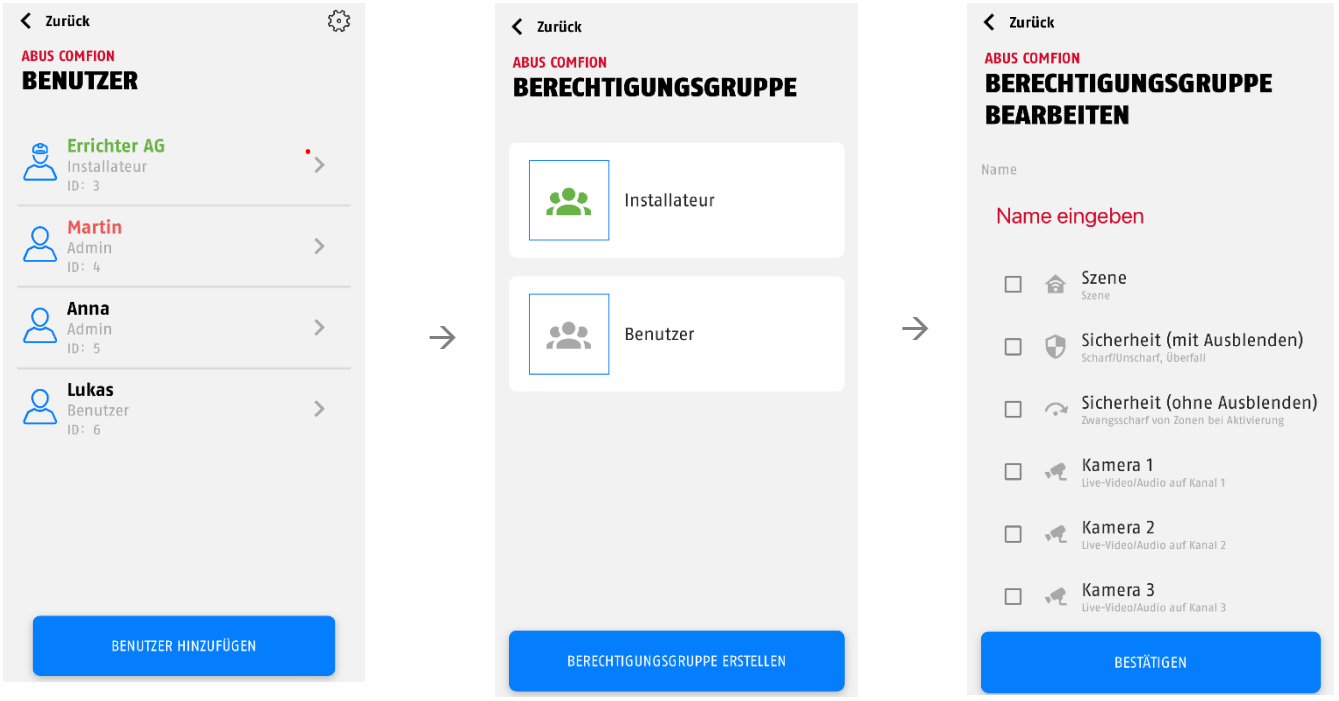
4.1. Uitleg over de verschillende rollen

Installateur	De installateur heeft alle gebruikersrechten tijdens de eerste inbedrijfstelling. Na overdracht van het systeem behoudt de installateur alle configuratierechten. De eigenaar van het systeem kan de rechten van de installateur voor het live camerabeeld intrekken en de toegang tot het systeem volledig blokkeren.
Admin	De systeembeheerder heeft alle gebruikersrechten voor het systeem. Hij kan ook automatiseringen en scènes aanmaken en bewerken. De installateur heeft ook de mogelijkheid om de admin configuratierechten te geven, zodat deze de rechten van een installateur heeft.
Eigen rol (Door gebruiker gedefinieerd)	U hebt de mogelijkheid om uw eigen niet-admin gebruikersgroepen aan te maken en hun autorisaties vast te leggen (zie hieronder)
Eigenaar (extra rol)	De eigenaarsrol wordt automatisch toegewezen aan de eerste bestaande Admin op het systeem. De eigenaarsrol kan niet handmatig worden toegewezen. Naast de Admin-rechten heeft de eigenaar van het systeem de rechten om gebruikers toe te voegen, uit te nodigen en te verwijderen. De eigenaar van het systeem is rood gemarkeerd in de gebruikerslijst.

De volgende instelopties zijn beschikbaar:

- Toegang inschakelen: blokkeert/geeft toegang tot het systeem en pushmeldingen)
- Hoofdinstallateur: Definieert met welk installateursaccount het systeem is verbonden voor onderhoud op afstand (installateursportaal)

Gebruikersgroepen aanmaken:



4.2. Inbedrijfstelling

De autorisatietypes "Installateur" en "Admin" zijn momenteel beschikbaar in de fabrieksinstellingen van de centrale. Als het systeem in bedrijf wordt gesteld door een installateur, is de installateur in eerste instantie bevoegd voor alle functies in de centrale.

4.2.1. Overdracht aan de eigenaar

Nadat u als installateur de installatie van de centrale hebt voltooid, moet het systeem worden overgedragen aan de eindgebruiker. De eerste Admin die wordt uitgenodigd , wordt de eigenaar van het systeem. U kunt dit herkennen aan het feit dat deze gebruiker rood gemarkeerd is.
Nadat de eigenaar is uitgenodigd, verliest de installateur de rechten om gebruikers te bewerken en toe te voegen. Extra gebruikers moeten door de eigenaar worden toegevoegd.

4.3. Gebruikers uitnodigen/toevoegen

Nieuwe gebruikers kunnen na de overdracht alleen worden uitgenodigd door de eigenaar. De volgende mogelijkheden zijn beschikbaar bij het toevoegen van een nieuwe gebruiker:

- Nieuwe gebruiker uitnodigen
  - Een gebruiker uitnodigen op basis van het e-mailadres.
- Kiezen van mijn leden
  - Uitnodigen van een lid. Leden kunnen worden toegevoegd aan de persoonlijke ledenlijst in het overzicht van de centrale. (Zie **6.3.2 Leden**)
- Lokale gebruiker aanmaken
  - Maak een lokale gebruiker aan zonder Abus Cloud account en zonder de app te gebruiken. De lokale gebruiker kan een afstandsbediening en een code voor het bedieningspaneel toegewezen krijgen. Bovendien kunnen een telefoonnummer en e-mailadres opgeslagen worden voor kennisgevingen.

De autorisatie van de toe te voegen gebruiker kan eveneens worden geselecteerd. U kunt kiezen tussen Installateur, Admin en de gebruikersgroepen die u zelf hebt aangemaakt.

4.4. Gebruikers verwijderen

Er zijn twee manieren om gebruikers te verwijderen uit het centrale:

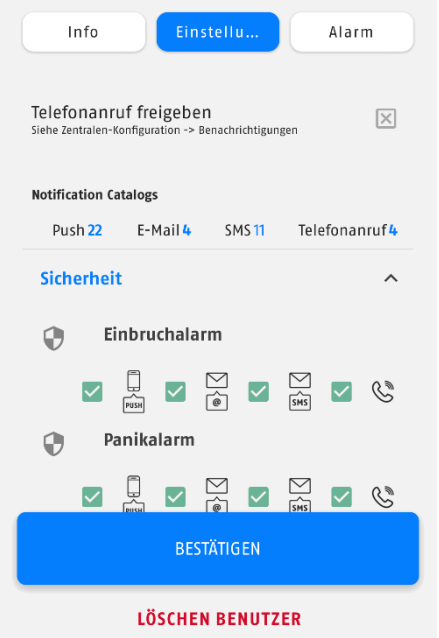
1. de eigenaar van het systeem (rood gemarkeerde gebruiker) kan elke andere gebruiker uit het systeem verwijderen door op deze gebruiker en de knop “Gebruiker verwijderen” te klikken.
2. Elke gebruiker kan zichzelf verwijderen uit het systeem door te klikken op de betreffende centrale in het overzicht van de centrale en deze ingedrukt te houden en vervolgens het verzoek tot verwijdering te bevestigen.

Aanwijzing	De eigenaar van het systeem kan zichzelf alleen op de tweede manier uit het systeem verwijderen (centrale verwijderen uit overzicht centrale). Zodra de eigenaar is verwijderd, gaat de rol terug naar de installateur. De installateur kan de nieuwe beheerder markeren als de nieuwe eigenaar door een nieuwe beheerder uit te nodigen.

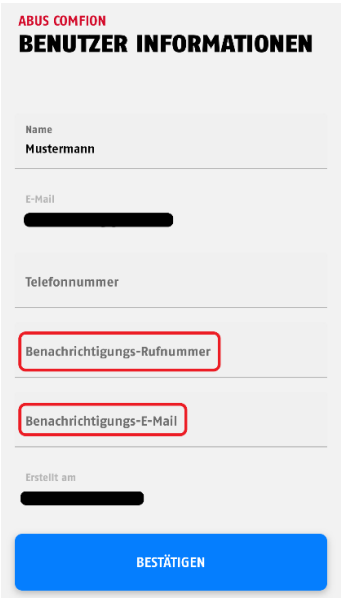
5. Communicatie

Het Comfion beveiligingssysteem heeft de volgende communicatiekanalen: Activering via e-mail, push, sms, telefoon en meldkamerbijschakeling

Onder het menupunt "Gebruikers" kunt u voor elke aangemaakte gebruiker selecteren welke kennisgevingen moeten worden verzonden voor elke gebeurtenis.



Uw telefoonnummer voor SMS & telefoongesprekken en uw e-mailadres voor kennisgevingen worden opgeslagen in uw account. U kunt deze op elk moment wijzigen. Ga hiervoor naar het overzicht van uw centrale en klik op het tandwieltje in de rechterbovenhoek. U kunt nu het telefoonnummer voor de kennisgevingen (**voer de landcode in, bijvoorbeeld +31**), en de e-mail voor kennisgevingen toewijzen.



5.1. Mobiele module

Het Comfion-beveiligingssysteem heeft een geïntegreerde mobiele module (2G/3G/4G). Deze kan worden gebruikt om tekstberichten te verzenden en te bellen in geval van een alarm. Het biedt bovendien een redundantiepad voor de volledige communicatie van het systeem. Dit betekent dat bij uitval van uw internetverbinding alle communicatie met de cloud, inclusief externe toegang en pushmeldingen, wordt afgehandeld via de mobiele telefoonmodus.

Tip	Schakel uw SIM-kaart pin-vrij voordat u deze in de mobiele module inlegt. U kunt de PIN meestal uitschakelen in de instellingen van elke mobiele telefoon.

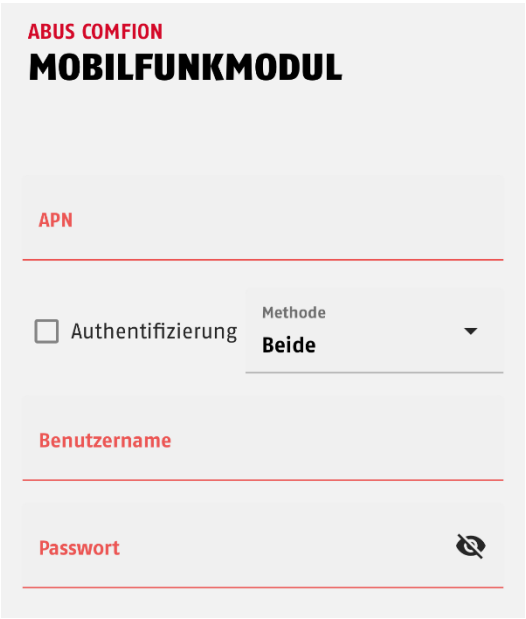
Tip	Gebruik geen SIM-kaarten uit het buitenland voor permanent gebruik in de Comfion.

Er is een SIM-kaart nodig om de mobiele modus te gebruiken. Deze SIM-kaart is vrij te kiezen (aanbeveling ABUS: Telekom, Vodafone, o2) en moet beschikken over de functies die u wilt gebruiken bij de centrale. Als u alle functies wilt gebruiken, hebt u een simkaart met sms, spraaktarief en datavolume nodig.

Tip	ABUS raadt het gebruik van prepaid kaarten in het Comfion beveiligingssysteem af vanwege bedenkingen over de betrouwbaarheid. Bovendien is het gebruik van Multi-SIMs niet aan te raden omdat dit kan leiden tot verbindingsproblemen.

RSSI-waarde	Bedeutung
-109 tot -95	Slecht
-93 tot -85	Laag
-83 tot -75	Goed
-73 tot -53	Uitstekend

In de mobiele module zelf hoeven geen verdere instellingen te worden verricht voor het verzenden van SMS-berichten of voor de belfunctie. Als u de redundantie van de netwerkdiensten wilt gebruiken, is het noodzakelijk om de APN-gegevens van de gebruikte SIM-kaart op te slaan. Het menu-item is te vinden onder "Centrale-configuratie" -> Tandwiel-icoon -> - "Modem".



De APN-gegevens van uw mobiele telefonieprovider zijn bijgevoegd bij uw SIM-kaart. U kunt deze alternatief ook online opvragen. De gegevens zijn niet SIM-kaart-specifiek, maar hetzelfde voor elke provider. Als een gebruikersnaam en wachtwoord zijn opgegeven in de APN-gegevens, vink dan het vakje "Authenticatie" aan.

Voorbeeld vodafone:

- APN: web.vodafone.nl
- Gebruikersnaam: vodafone
- Wachtwoord: vodafone

5.2. E-mail

Het versturen van e-mails vanuit Comfion werkt zonder configuratie en wordt afgehandeld via de cloud.

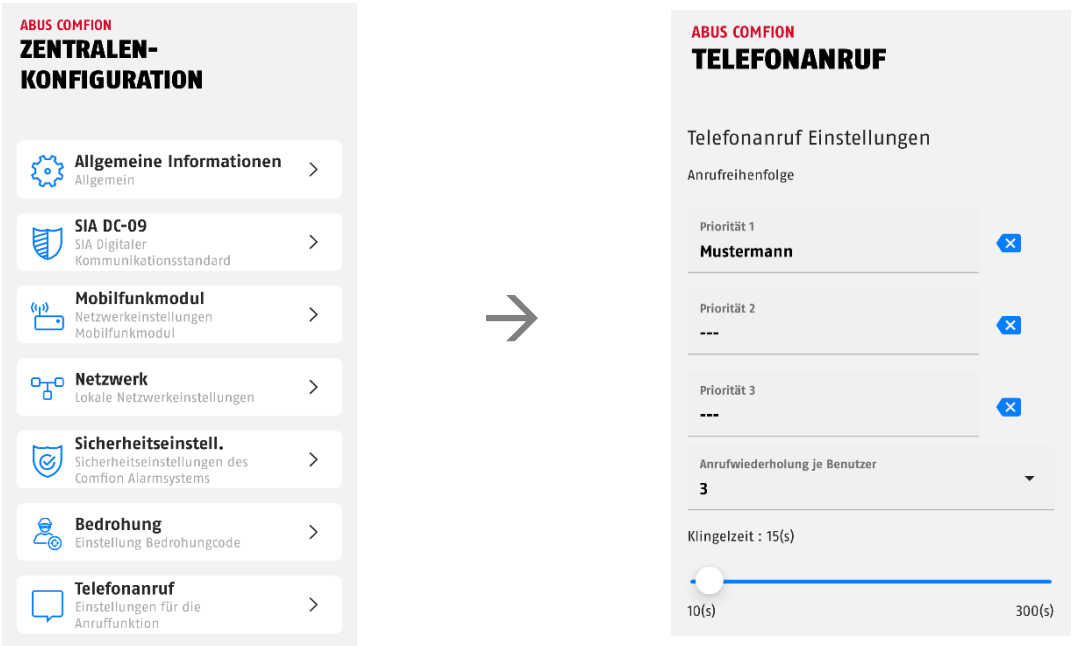
Als het e-mailadres dat moet worden verwittigd anders is dan het e-mailadres van je account, kun je een notificatieadres opslaan in je account (zie **5. Communicatie**). Als u geen notificatie-e-mail invult, worden de e-mails naar uw accountadres gestuurd.

5.3. Telefonische oproep

Het Comfion-beveiligingssysteem kan u opbellen bij een alarm. Het systeem heeft geen spraakkiezer, wat betekent dat er geen spraakbericht wordt afgespeeld bij deze oproep. De beloproep is alleen bedoeld als waarschuwing en moet de gebelde gebruiker op de hoogte brengen van een alarm. Het type alarm kan worden afgelezen aan de pushmelding die tegelijkertijd wordt verzonden.

Voor de belfunctie is een SIM-kaart met belfunctie en voldoende belkrediet vereist. Meer informatie over de mobiele module vindt u onder **5.1 Mobiele module**.

- Om beloproepen te ontvangen, moet het telefoonnummer van de ontvanger opgeslagen zijn in het gebruikersaccount (zie **5.** Communicatie).
- U moet ook de oproepvolgorde definiëren onder "Centrale-configuratie" -> Tandwiel-icoon -> "Telefonische oproep". Er kunnen maximaal 3 gebruikers achter elkaar worden gebeld.



Aanwijzing	De herhalingen van oproepen per gebruiker zijn standaard ingesteld op 3. Dit betekent dat elke beller drie oproepen ontvangt. De oproep kan niet worden bevestigd.

5.4. SMS

Het Comfion-systeem kan sms-berichten herkennen aan de hand van de gebeurtenissenlijst (zie **5. Communicatie**). U kunt ook automatiseringen gebruiken om sms-berichten te versturen met vrij definieerbare tekst voor elke gebeurtenis.

Om sms-berichten te kunnen versturen, moet er een SIM-kaart in de module worden geplaatst en moet het kennisgevingsnummer in het account worden opgeslagen (zie **5. Communicatie**).

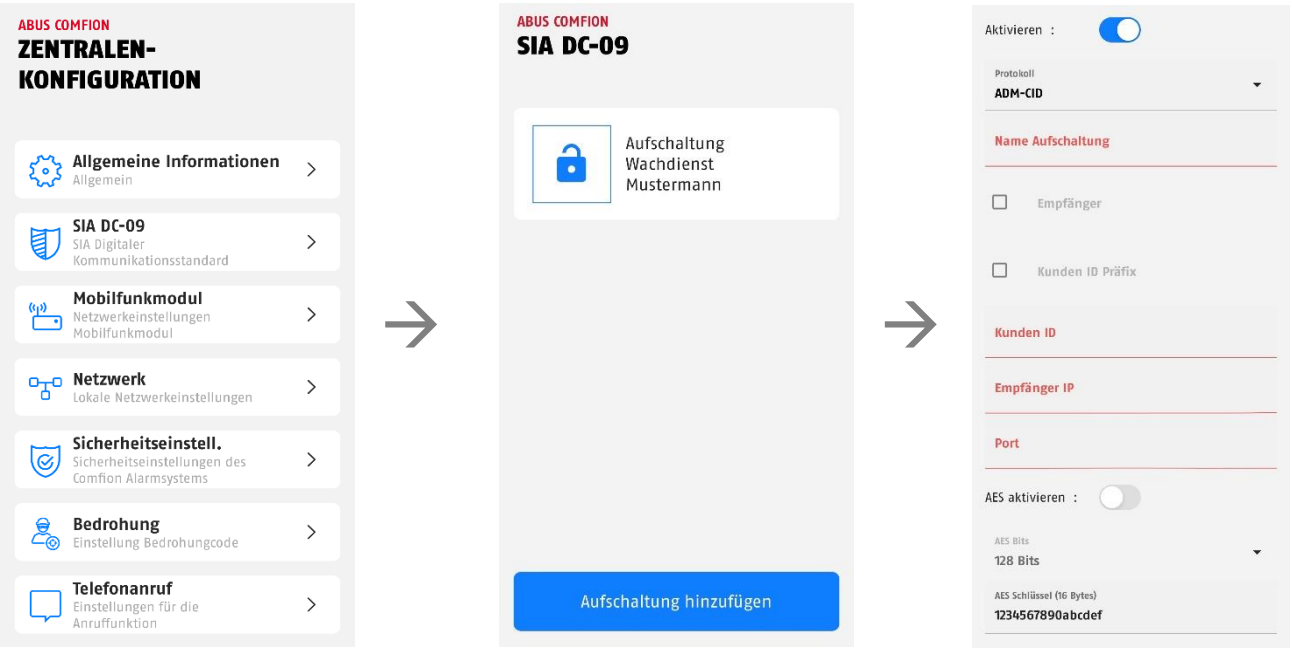
5.5. SIA DC-09 (meldkamer bijschakelen)

Het Comfion draadloze beveiligingssysteem heeft een digitale meldkamerkiezer die het Contact-ID protocol kan verzenden via de SIA DC-09 standaard. U kunt meerdere bijschakelingen tegelijk configureren en zo communiceren met diverse beveiligingsdiensten.

Voer de gegevens die u van uw dienstverlener hebt ontvangen in de relevante velden in. De twee grijze velden "Ontvanger" en "Klant-ID prefix" zijn over het algemeen niet vereist en hoeven alleen te worden geactiveerd als uw dienstverlener hier expliciet om vraagt.

Je kunt kiezen tussen de volgende opties in het veld “Statisch testbericht”:

- **DC-09 Lijnbewaking** -> Bewaking geïntegreerd in het protocol van de centrale (moet worden ondersteund door de centrale)
- **CID-testbericht 602** -> Verzending van de contact-ID-code 602 met het ingestelde interval



Je krijgt toegang tot de geavanceerde instellingen via het tandwielsymbool in de rechterbovenhoek van het scherm. Hier kun je het statische testbericht activeren en het interval instellen.

6. Algemene informatie, onderhoud en opmerkingen

6.1. Centrale-configuratie

Onder het menu-item Centrale-configuratie vindt u alle belangrijke informatie over uw centrale en kunt u ook belangrijke instellingen voor het systeem maken

Nadat u het menu-item Centrale-configuratie hebt opgeroepen, ziet u de volgende informatie:

- Centrale-naam (invoerveld)
- Symbool (kan worden vervangen door eigen foto)
- Netwerk (weergave van het type netwerkverbinding)
- Status mobiel netwerk (drop-down)
  - Moduletype (ingebouwde mobiele telefonie-chip)
  - SIM-kaart (aanduiding of ingelegd)
  - IMEI nummer
  - Telefoongesprek (weergave of mogelijk met ingelegde SIM)
  - Verbinding (weergave via verbindingsstatus)
  - Signaalsterkte (dBm)
- Stroomvoorziening (weergave adapter of batterij)
- Firmware (klikken om de versie en release-notes weer te geven)
- RF module (weergave van de FW van de draadloze module)
- Locatie
- Artikelnummer

U kunt meer instellingenmenu's openen via het tandwielsymbool rechtsboven. De instellingen voor SIA DC-09, telefoonoproep en de mobiele module zijn te vinden onder 5. Communicatie.

6.1.1. Algemene informatie

Informatie over het geplaatste opslagmedium (harde schijf of SD-kaart) wordt weergegeven onder de kop "Geheugen".

De gebruikte tijdzone en de NTP-server worden weergegeven onder de kop "Datum en tijd".

Je kunt het systeem opnieuw opstarten met de knop “Herstarten”.

6.1.2. Netwerk

In dit menu kunt u de netwerkinstellingen bekijken en indien nodig aanpassen.

U kunt kiezen uit drie methoden:
DHCP (standaard): Dynamic Host Configuration Protocol is een client/server-protocol waarbij de Comfion automatisch wordt voorzien van zijn IP-adres en andere bijbehorende informatie door de router.

PPPoE: Point-to-Point Protocol over Ethernet is een netwerkprotocol dat een directe verbinding binnen het interne netwerk beschikbaar stelt. Hiervoor is authenticatie met gebruikersnaam en wachtwoord vereist.

Statisch: Als "Statisch" is geselecteerd, worden de Comfion-netwerkgegevens handmatig toegewezen. Bespreek dit met de netwerkbeheerder en wijs geen IP-adres toe uit de DHCP-pool.

Aanwijzing	Onjuiste IP-instellingen betekenen dat uw systeem geen verbinding kan maken met het netwerk, waardoor het niet bereikbaar is voor de app. Druk in dit geval 6 seconden op de knop "connect" op de achterkant van het systeem en laat deze vervolgens los. De centrale zal dan opnieuw opstarten en de netwerkinstellingen terugzetten naar de standaard DHCP-instellingen.

6.1.3. Beveiligingsinstellingen

Onderhoudsmodus	Aan/Uit (Standaard uitgeschakeld)	De onderhoudsmodus wordt gebruikt om het systeem te installeren en te onderhouden. Het systeem kan geen alarmen activeren wanneer de onderhoudsmodus actief is.
Zoneblokkering	3x-20x (Standaard 5x)	Als een zone vaker wordt getriggerd dan ingesteld, zal deze zone niet meer triggeren totdat de alarmen uit de alarmgeschiedenis zijn verwijderd.
Max. aantal herhalingen van toetsenveldinvoer	3x-20x (Standaard 5x)	Geeft aan na hoeveel onjuiste PIN-invoer op het bedieningspaneel het is vergrendeld
Time-out bediendeel	5-180 sec (Standaard 30 sec)	Tijdsinstelling voor hoe lang het bedieningspaneel wordt vergrendeld na X onjuiste invoer
Ingangsvertraging	5-45 sec (Standaard 10 sec)	Als het systeem ingeschakeld is, wordt de ingangsvertraging geactiveerd door een ingang of ingang/uitgangszone
Uitgangsvertraging	5-45 sec (Standaard 30 sec)	Tijd voordat het controlecentrum overschakelt naar de bewapende status
Vertraging bij transmissie	5-180 sec (Standaard 60 sec)	Als deze functie is geactiveerd in de zone, wordt het verzenden van een trigger vertraagd met de ingestelde tijd.
Stroomuitval Vertraging	0-30 min (Standaard 0 min)	Instelbare vertraging voor het signaleren van spanningsverlies (12V DC)
Inbraaksirene activeren	Aan/Uit (Standaard AN)	Inschakeling sirene bij inbraakalarm
Sireneduur inbraakalarm	5-180 sec (Standaard 60 sec)	Duur van de akoestische signalering door in het systeem geïntegreerde sirenes
Sabotagesirene activeren	Aan/Uit (Standaard AN)	Inschakeling sirene bij sabotagealarm
Sabotagealarm sireneduur	5-180 sec (Standaard 60 sec)	Duur van de akoestische signalering door in het systeem geïntegreerde sirenes
Paniekalarm sirene activeren	Aan/Uit (Standaard uitgeschakeld)	Inschakeling van de sirene bij een overvalalarm
Sireneduur paniekalarm	5-180 sec (Standaard 60 sec)	Duur van akoestische signalering door in het systeem geïntegreerde sirenes
Activeer wateralarmsirene	Aan/Uit (Standaard AN)	Inschakeling sirene bij wateralarm
Sireneduur wateralarmsirene	5-180 sec (Standaard 60 sec)	Duur van akoestische signalering door in het systeem geïntegreerde sirenes
Brandalarmsirene activeren	Aan/Uit (Standaard AN)	Inschakeling sirene bij brandalarm
Duur van brandalarmsirene	5-180 sec (Standaard 60 sec)	Duur van akoestische signalering door in het systeem geïntegreerde sirenes
SOS-sirene activeren	Aan/Uit (Standaard uitgeschakeld)	Sireneactivering bij een overvalalarm via de app
SOS-Sireneduur	5-180 sec (Standaard 60 sec)	Duur van de akoestische signalering door in het systeem geïntegreerde sirenes
Netwerkfout overbruggen	Aan/Uit (Standaard uitgeschakeld)	Detectie en rapportage van een netwerkfout
Accu-fout overbruggen	Aan/Uit (Standaard uitgeschakeld)	Een batterijstoring herkennen en melden
Overbruggen stroomverlies	Aan/Uit (Standaard uitgeschakeld)	Detectie en signalering van stroomverlies (12V DC)
Overbruggen dekelsabotage rechts	Aan/Uit (Standaard uitgeschakeld)	Detectie en signalering van sabotage van de rechterklep (harde schijf)
Overbruggen dekelsabotage links	Aan/Uit (Standaard uitgeschakeld)	Detectie en signalering van sabotage van de linkerklep (batterij)

6.1.4.Centrale back-up

Aanwijzing	Om veiligheidsredenen wordt het back-up bestand van je alarmpaneel volledig versleuteld opgeslagen in de Abus Cloud, uitsluitend op Europese servers.

Back-up maken
Onder het menu-item Back-up in de centrale configuratie kunt u handmatig een back-up maken en de automatische back-up activeren. De automatische back-up wordt wekelijks uitgevoerd.

Een back-up importeren
Om de back-up in een nieuw alarmpaneel te importeren, gaat u als volgt te werk:

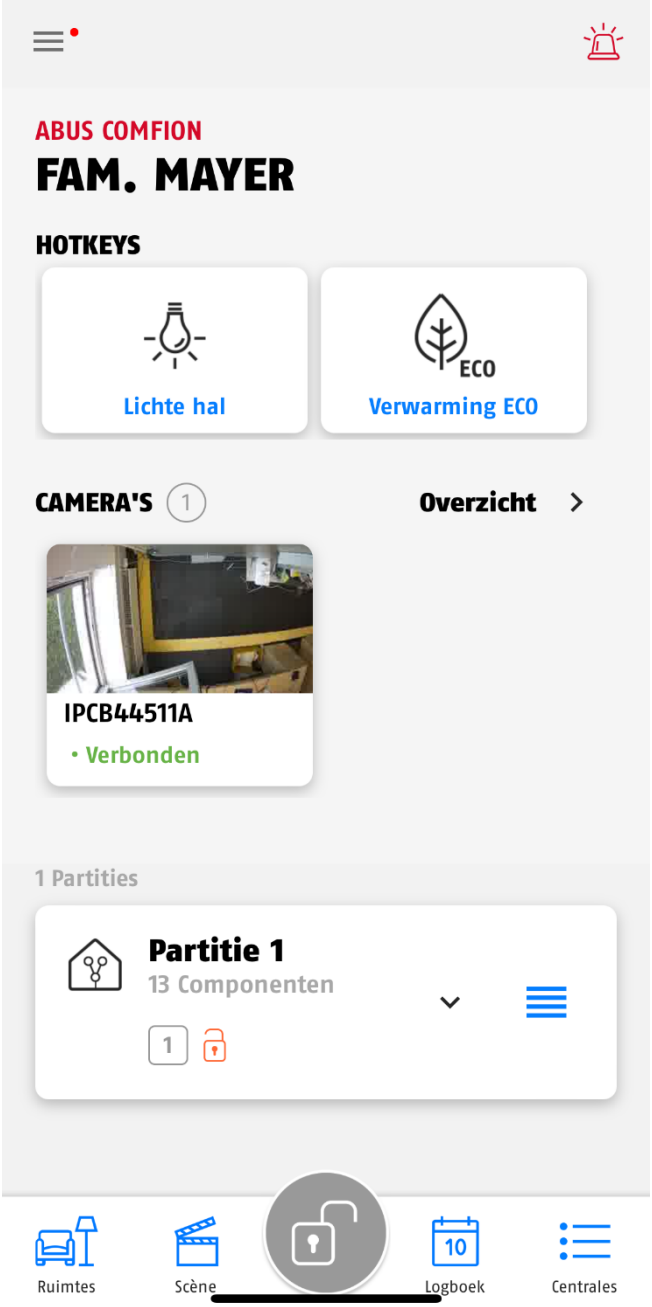
1. Koppel het alarmpaneel waarvan de back-up afkomstig is los van het netwerk, als u dit nog niet hebt gedaan, en schakel het uit.
2. Klik in het centrale overzicht in de app op het + symbool om een nieuwe centrale toe te voegen
3. Selecteer "Back-up importeren
4. Scan de QR-code op de achterkant van uw nieuwe alarmcentrale
5. Selecteer het alarmpaneel waarvan u de back-up wilt laden
   Opmerking: Na het importeren wordt de back-up verwijderd uit de cloud en werken de componenten niet meer op het oude alarmpaneel.
6. Voer de gewenste centrale naam in van uw nieuwe centrale
7. Na bevestiging wordt er een verificatiecode verzonden naar het e-mailadres van de eigenaar van het systeem. Voer deze code in de app in en klik op "Start import".
8. De import wordt nu uitgevoerd. Je kunt nu de app sluiten en wachten tot je de pushmelding krijgt dat het alarmpaneel online is en de stroomvoorziening beschikbaar is.

Om een configuratie te herstellen naar dezelfde hardware (centrale), gaat u als volgt te werk:

1. Reset het betreffende alarmpaneel naar de fabrieksinstellingen (druk 10 seconden op de resetknop -> zie 6.5.1)
2. Ga naar het overzicht van de centrale in de app en klik op het + symbool om een nieuwe centrale toe te voegen
3. Selecteer "Herstellen".
4. Scan de QR-code op de achterkant van uw alarmcentrale
5. Voer de gewenste centrumnaam van uw centrale in
6. De import wordt nu uitgevoerd. Je kunt nu de app sluiten en wachten tot je de pushmelding krijgt dat het alarmpaneel online is en de stroomvoorziening beschikbaar is.

6.2. Dashboard

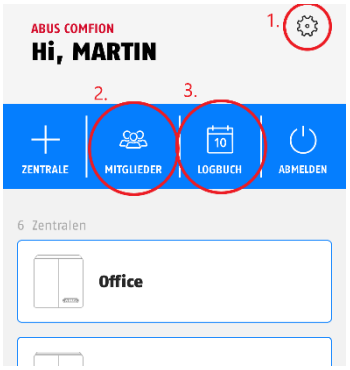
U kunt het systeem bedienen via het Dashboard en ook een groot deel van uw werk als installateur uitvoeren.



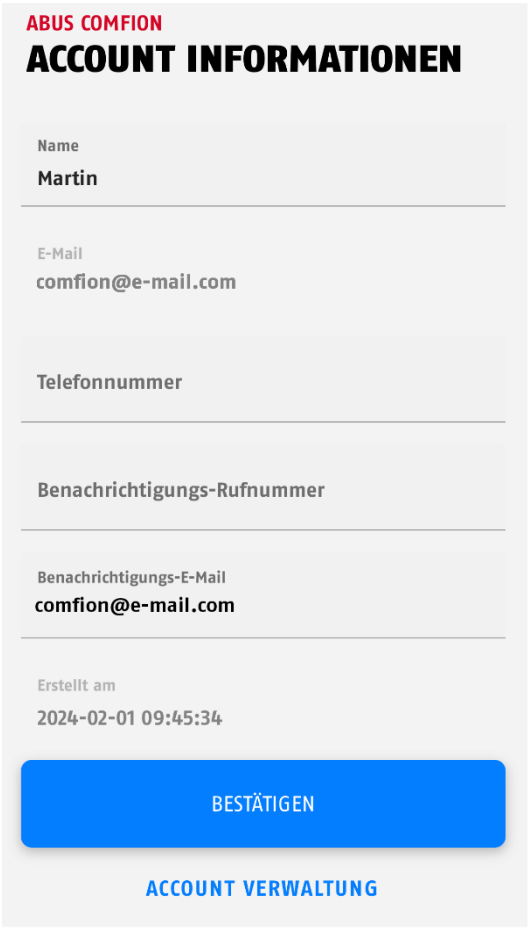
- Menuoproep & paniekknop
- Centrale naam
- Hotkeys - Kunnen worden gedefinieerd onder "Scènes"
- Camera-overzicht - toegang tot livestreams van camera's en algemene camera-instellingen
- Cameraselectie - Klik op de betreffende camera om de livestream van de camera direct te openen
- Partitieweergave. De partitie kan worden bewerkt na een lange klik. Klik kort om de partitie open te klappen en de toegewezen componenten weer te geven
- Ruimtes = Weergave van het ruimteoverzicht & componenten
- Scène = Scènes & automatiseringen
- Logboek = Weergave van het gebeurtenissengeheugen
- Centrales = Overzicht Centrales

6.3. Centrale-overzicht

In het centrale-overzicht van het systeem kunt u naast het toevoegen van nieuwe centrales de bestaande centrales bekijken en openen, uw accountgegevens bewerken (1), uw leden beheren (2) en het account-logboek bekijken (3).



6.3.1. Informatie voor de gebruiker



- ➔ Naam (weergegeven in centrale & logboek)
- ➔ E-mail
- ➔ Telefoonnummer

Telefoonnummer voor notificatie

- ➔ Notificatie e-mail voor verzending per e-mail vanuit de centrale
- ➔ Tijdstip waarop het account is aangemaakt
- ➔ Bevestigingsknop om de invoer op te slaan
- ➔ In-app verwijderfunctie van het ABUS-account

6.3.2. Leden

In de Comfion-app kunt u een ledenlijst bijhouden. Dit is puur optioneel en is niet vereist om de Comfion-systemen te kunnen gebruiken. Met de ledenlijst kunt u bij het toevoegen/uitnodigen van nieuwe gebruikers in een centrale deze heel eenvoudig uit uw leden selecteren.

6.3.3. Accountlogboek

Alle berichten van systemen met geautoriseerde toegang worden vermeld in het accountlogboek. Als de toegang tot een systeem is geblokkeerd, worden logboekvermeldingen van dit centrale niet opgeslagen in het accountlogboek.

6.4. Automatiseringen & scènes

Het Comfion-systeem biedt u de mogelijkheid om tot 100 scenario's te configureren. Deze scènes of automatiseringen kunnen volledig vrij worden ingesteld, waardoor u maximale flexibiliteit hebt.

U kunt zowel scènes als automatiseringen toevoegen onder het tabblad "Scènes".

Opgelet	Er mogen geen automatiseringen worden aangemaakt die elkaar tegenspreken of in een cirkel oproepen plegen. Dit kan leiden tot ernstige werkingsproblemen bij de centrale.

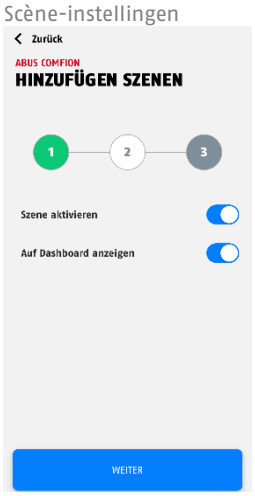
Opgelet	Zorg ervoor dat u een interval van minstens 5 seconden laat tussen twee schakelcommando's voor hetzelfde apparaat om een vlotte werking te garanderen.

Scène = Actie wordt getriggerd door een gebruiker via de app (Hotkey). Kan worden weergegeven in het dashboard.
Voorbeeld: Contactdoos AAN/UIT via app

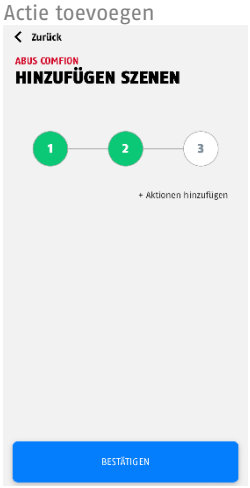
Voorbeeldconfiguratie van een scène:

Naam / symbooltoewijzing

Scène-instellingen



Actie toevoegen



Actieselectie

Automatisering = Bestaat altijd uit een gedeelte als.... dan .... Vrij configureerbaar.
Voorbeeld: Wanneer het systeem ingeschakeld is, dan het licht uit

In het indien-deel kunt u kiezen tussen een EN-kopeling en een OF-koppeling. Met de EN-koppeling moet aan ALLE voorwaarden worden voldaan om de actie uit te voeren. Er moet aan minstens EEN voorwaarde zijn voldaan om de actie uit te voeren bij de OF-koppeling.

In het Als-gedeelte kunt u kiezen uit de volgende categorieën voor de gebeurtenissen:

- Systeem -> Hier vindt u systeemgebeurtenissen zoals een stroomstoring, maar ook het tijdschema
- Partitie -> Partitiegebeurtenissen zoals in-/uitschakelen, inbraak, gereed voor inschakeling en nog veel meer zijn hier te vinden
- Zone -> Alle zone-gerelateerde gebeurtenissen kunnen hier worden gevonden (bijv. zone-inbraak)
- Ruimte -> Alle componenten en de bijbehorende gebeurtenissen kunnen hier worden gevonden (bijv. openingsmeldercontact geopend of knop van wandschakelaar ingedrukt)

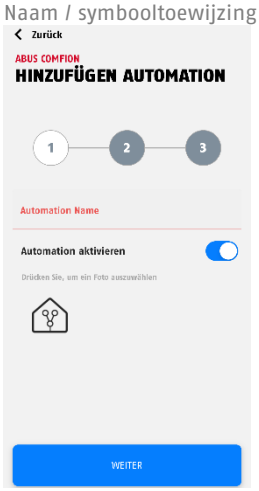
- Uitleg "Uitgebreid":
  Onder "Uitgebreid" kunt u een tijd instellen die bepaalt hoe lang aan de ingestelde voorwaarden voldaan moet zijn, voordat de actie wordt uitgevoerd. De actie wordt alleen uitgevoerd als aan de voorwaarden voor de ingestelde tijdsperiode is voldaan en deze niet meer veranderen.
  Voorbeeld: Als de deur 30 seconden open is, verzend dan een pushmelding

In het Dan-gedeelte wordt onderscheid gemaakt tussen

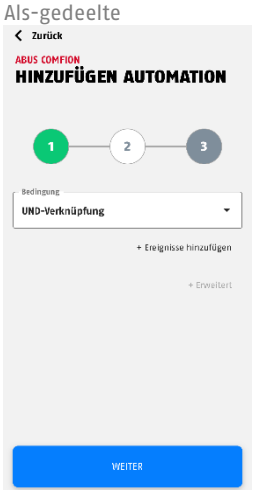
- "Als, dan" -> Actie wordt uitgevoerd als de voorwaarden in het Als-gedeelte van toepassing zijn
- "Als voorbij, dan" -> actie wordt uitgevoerd als de voorwaarden in het "Als"-gedeelte niet langer van toepassing zijn

Voorbeeldconfiguratie van een automatisering:

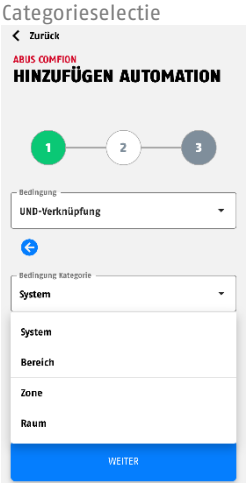
Naam / symbooltoewijzing



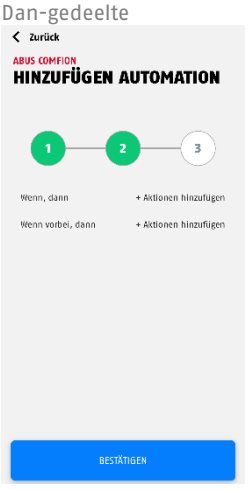
Als-gedeelte



Categorieselectie



Dan-gedeelte



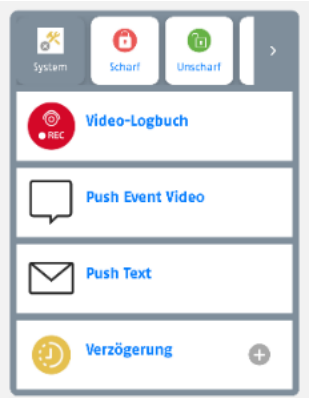
De volgende actieselecties zijn beschikbaar wanneer "Systeem" wordt geselecteerd in het Dan-gedeelte van scènes of automatiseringen:

Videologboek: Aanmaken van een logboek-item (15 sec) met een uitsnede van de camera-opname.

Push-event video: Een pushbericht verzenden met definieerbare tekst en een uitsnede (15 sec) van de camera-opname.

Push-tekst: Een pushbericht verzenden met definieerbare tekst.

Vertraging: Instelbare vertraging in seconden - bijvoorbeeld tussen twee acties



6.5. Resets

6.5.1. Fabrieksreset

Om het systeem terug te zetten naar de fabrieksinstellingen, houdt u de resetknop (zie 2.3 Beschrijving van het apparaat) >10 seconden ingedrukt en laat u hem weer los. De LED's van de centrale gaan na een paar seconden uit en het systeem start opnieuw op. Na de herstart wordt het alarmpaneel teruggezet naar de fabrieksinstellingen en kan het opnieuw worden ingesteld.

6.5.2. Gebruiker reset

Om de gebruikers van het alarmpaneel te resetten of alle gebruikers uit het systeem te verwijderen, drukt u binnen 5 seconden 5 keer op het linker sabotagecontact (boven de resetknop). Na enkele seconden schakelt de internet-LED kort over naar rood. Je moet een pushmelding ontvangen op de aangesloten apparaten dat het betreffende centrale is verwijderd.

Als alle LED's weer groen zijn (de internet-LED kan groen knipperen), kun je het systeem weer toevoegen met het +-symbool in je app.

6.5.3. Netwerk reset

Als je je systeem niet meer kunt bereiken in het netwerk vanwege onjuiste IP-instellingen, is het mogelijk om de centrale terug te zetten naar DHCP. Houd hiervoor de resetknop voor het netwerk op de achterkant van de centrale (met het label “Connect”) 6 seconden ingedrukt. Na een paar minuten zou het systeem weer toegankelijk moeten zijn.

6.6. Werking van de LED's

Aanwijzing	De onderstaande LED-indicaties gelden pas na de eerste inbedrijfstelling van het systeem

Voedings-LED: Geeft de spanningsstatus aan en kan fouten signaleren

Kleur	Betekenis
Groen	Netvoedingsspanning
Rood	Batterijvoeding
Oranje	Firmware-update

Internet LED (Globe): Geeft de status van de cloudverbinding weer

Kleur	Betekenis
Groen	Verbonden met de cloud (Eigenaar is aangemaakt)
Rood	Verbinding met de cloud mislukt
Knippert groen	Verbonden met de cloud (Geen eigenaar aangemaakt)

Netwerk-LED (pijlen): Toont het communicatiekanaal dat momenteel in gebruik is

Kleur	Betekenis
Groen	Verbonden met internet via LAN
Rood	3G/4G-verbinding

Status-LED (slot): Geeft systeemstatus weer

Kleur	Betekenis
Rood	Systeem ingeschakeld
Oranje	Systeem gedeeltelijk ingeschakeld
Groen	Systeem uitgeschakeld
Knippert groen	Centrale maakt verbinding met component

6.7. Operatie

6.7.1. Inschakelen / Uitschakelen

- APP: In-/uitschakelen kan worden uitgevoerd in de app door de alarmmodi uit te voeren. Klik hiervoor op de centrale knop onderaan het dashboard (slotsymbool) en selecteer vervolgens de actie (bijv. volledig inschakelen).
- KEYPAD: Je kunt het systeem in- en uitschakelen met een draadloos toetsenbord. Voer hiervoor je gebruikerscode in en klik vervolgens op de knop (vergrendelknoppen). Meer gedetailleerde informatie vind je in de gebruikershandleiding of in de handleiding van het toetsenbord.
- KEYFOB: Je kunt de alarmmodi toewijzen aan de knoppen op je draadloze afstandsbediening en de betreffende actie uitvoeren door op een knop te drukken. De instelling vind je onder de keyfob.
- AUTOMATISERING: Je kunt automatisering gebruiken om het in- of uitschakelen van het systeem te koppelen aan omstandigheden. Dit kan bijvoorbeeld worden gebruikt om te schakelen volgens een schema of wanneer een draadingang wordt geactiveerd.

6.7.2. Een alarm resetten

Het Comfion-systeem moet door de gebruiker worden hersteld na een alarm (inbraak, sabotage, enz.):

- Het Comfion-systeem herstelt het alarm automatisch wanneer het wordt uitgeschakeld. Zodra alle geactiveerde detectoren weer de normale status hebben, verdwijnt het waarschuwingsoverzicht van het dashboard.

6.8. Verklaring van symbolen

	Component geactiveerd (bijv. raam open)
	Sabotage (bijv. melderbehuizing geopend)
	Component aangestuurd (bijv. sirenegeluid geactiveerd)
	Componentstatus UIT (bijv. radio-contactdoos uit)
	Componentstatus AAN (bijv. radio-contactdoos aan)
	Beweging herkend
	PIR-camera: 1 Foto maken (activeringstoets) 2 Opname wordt gemaakt 3 Opname wordt verzonden
	Kabelbreuk (bijv. 3in1 melder)
	Voedingspanning aangesloten
	Draadloze verbinding onderbroken
	Zone gesloten
	Zone open
	Laadstatus batterij
	4 streepjes = uitstekend 3 streepjes = zeer goed 2 streepjes = goed 1 streepje = OK 0 streepjes = slecht

6.9. ABUS Cloud

Het Comfion beveiligingssysteem maakt verbinding met de Abus Cloud tijdens de eerste ingebruikname. Het systeem wordt ook opgeslagen in het Abus Cloud-installateursaccount van de installateur. Als dit niet gewenst is, kan het vakje "Hoofdinstallateur" worden uitgeschakeld onder de betreffende gebruiker in het systeem, of kan een andere installateur worden geselecteerd.

6.10. Opmerkingen over de harde schijf

- De schroeven voor de bevestiging van de harde schijf mogen alleen met de hand worden vastgedraaid
- De levensduur van de batterij van de centrale hangt onder andere af van de geïnstalleerde harde schijf en het energieverbruik daarvan, maar ook van het aantal camera's en het geselecteerde opnametype (continu opnemen, enz.).
- De harde schijf die in de Comfion is geïnstalleerd, moet zijn geformatteerd in exFAT- of NTFS-formaat
- Vervang de harde schijf alleen als het bedieningspaneel spanningsvrij is

6.11. Onderhoud en onderhoud door installateurs

Test tijdens het routine-onderhoud of het systeem goed werkt:

- Controleer de Comfion op duidelijke tekenen van schade aan de behuizing of de frontafdekkingen.
- Controleer de werking van de sabotageschakelaars (wandafscheuring/behuizingsdeksel links, behuizingsdeksel rechts)
- Controleer de toestand van de noodstroomaccu
- Maak de behuizing schoon
    - Gelieve de oppervlakken met een droge, zachte doek schoon te vegen.
    - Gebruik geen water of oplos- of reinigingsmiddelen.
- Controleer de signaalsterkte en de status van de batterij/oplaadbare batterij van alle componenten
- Vervang de batterijen of accu's zoals aanbevolen in de instructies van de fabrikant
- Test elke component.
- Reinig voorzichtig de objectieven van alle PIR-melders en camera's met een schone, droge, zachte doek.
    - Gebruik geen water of oplos- of reinigingsmiddelen.
- Voer een looptest uit van alle melders.
- Test alle signaalgevers
- Test de communicatie.

Aanwijzing	De onderstaande LED-indicaties gelden pas na de eerste inbedrijfstelling van het systeem

Hoe vervang ik de accu van de centrale:

- Zet de centrale in de onderhoudsmodus (beveiligingsinstellingen)
- Open het linker behuizingsdeksel
- Koppel de voeding en de oude accu los van de centrale
- Wacht 30 seconden
- Sluit de nieuwe accu en de spanningsvoorziening weer aan
- Sluit de klep van het systeem en verlaat de onderhoudsmodus weer

6.12. Tabel met radiosignaalsterkten

RSSI-Waarde (dBm)	Betekenis	Weergave op component
<= -100	Slecht	0 Bar
<= -96	OK	1 Bar
<= -91	Goed	2 Bar
<= -86	Zeer goed	3 Bar
> -86	Uitstekend	4 Bar

7. Geschiedenis van de release

7.1. Overzicht

publicatiedatum	Firmware-Versie Centrale	App Versie IOS/Android
21.03.2024	1.0.4736	0.2.1360
26.03.2024	1.0.4751	onveranderd
10.05.2024	1.0.4957	0.3.1401
02.07.2024	1.0.5150	0.5.1471
16.09.2024	1.0.5398	0.5.1575 / 0.5.1577
11.11.2024	1.0.5500	0.6.1626
15.11.2024	1.0.5510	Onveranderd
18.02.2025	1.0.5727	0.6.1702
28.02.2025	1.0.5782	Onveranderd
18.03.2025	1.0.5836	Onveranderd

7.2. Release notes

De release notes voor de huidige firmware-update zijn te vinden in je Comfion-app of onder de volgende link:
https://l.ead.me/becYdV

8. Garantie

- ABUS-producten zijn met de grootst mogelijk zorgvuldigheid ontworpen, geproduceerd en op basis van de geldende voorschriften getest.
- De garantie heeft uitsluitend betrekking op gebreken die op materiaal- of fabrieksfouten duiden op het moment van verkoop. Bij bewijs van een materiaal- of fabrieksfout wordt de module naar keuze van de garantiegever gerepareerd of vervangen.
- De garantie eindigt in dit geval met het aflopen van de oorspronkelijke garantieperiode van 2 jaar. Verdergaande aanspraken zijn uitdrukkelijk uitgesloten.
- ABUS is niet aansprakelijk voor defecten en schade veroorzaakt door invloeden van buitenaf (bijv. transport, gebruik van geweld, onjuiste bediening), onjuist gebruik, normale slijtage of het niet in acht nemen van deze instructies en de onderhoudsvoorschriften.
- Bij het indienen van een garantieclaim moet bij het product het originele aankoopbewijs met datum van de aankoop en een korte schriftelijke beschrijving van het gebrek worden gevoegd.
- Als u gebreken aan het product vaststelt, die bij de aankoop reeds aanwezig waren, wendt u zich binnen de eerste twee jaar direct aan uw leverancier.

9. Recyclen

Gooi het apparaat weg in overeenstemming met de EU-richtlijn 2012/19/EU voor afgedankte elektrische en elektronische apparatuur - WEEE (Waste Electrical and Electronic Equipment). Bij vragen wendt u zich tot de voor de afvoer bevoegde gemeentelijke dienst. Informatie over verzamelpunten voor afgedankte apparatuur krijgt u bij de gemeente, regionale afvalbedrijven of bij uw leverancier.

10. Conformiteit

10.1. EU-conformiteitsverklaring

ABUS Security Center GmbH & Co. KG verklaart hierbij dat de radioapparatuur van het type FUAA80000 voldoet aan Richtlijn 2014/53/EU en 2011/65/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: abus.com > Artikel zoeken > FUAA80000 > Downloads

10.2. Conformiteit aan EN 50131

Het FUAA80000 veiligheidssysteem is gecertificeerd voor veiligheidsniveau 2 wanneer het op de juiste manier is geïnstalleerd volgens EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 en EN 50131-5-3:2017.

ABUS | Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel: +49 82 07 959 90-0